УДК 327;930.22;007
ББК 66.4;73
Д00

Девятый международный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» и Одиннадцатая научная конференция Международного исследовательского консорциума информационной безопасности 20–23 апреля 2015 года. Гармиш-Партенкирхен, Германия. — М.: Издательство Московского университета, 2015. — 352 с.
ISBN 978-5-19-000000-0

В настоящем сборнике материалов Девятого международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» и Одиннадцатой научной конференции Международного исследовательского консорциума информационной безопасности представлены доклады ряда ведущих отечественных и зарубежных экспертов, занимающихся исследованиями вопросов информационной безопасности, кибербезопасности и международной информационной безопасности.

Ключевые слова: Информационная безопасность, кибербезопасность, международная информационная безопасность, защита критически важной инфраструктуры, международное право, международное гуманитарное право, киберконфликты, кибервойна.

УДК 327;930.22;007
ББК 66.4;73

ISBN 978-5-19-000000-0

Содержание

В.П.Шерстюк

Сопредседатель оргкомитета Форума, советник Секретаря Совета Безопасности Российской Федерации, директор Института проблем информационной безопасности МГУ имени М.В.Ломоносова

Вступительное слово О программе и задачах IX международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности»

Уважаемые участники конференции!

Дамы и господа!

Прежде всего, хотел бы выразить искреннюю признательность всем жителям города Гармиш-Партенкирхен, благодаря радушию которых эксперты в области информационной безопасности многих государств мира уже девятый год подряд могут собираться и обсуждать наиболее актуальные проблемы обеспечения международного мира и безопасности в условиях возрастания опасности злонамеренного использования информационных и коммуникационных технологий (ИКТ). Эти дискуссии будут проходить в обстановке определенного обострения международных отношений, произошедших за последний год, усиления политической нестабильности, затронувшей и информационное пространство. Сложившиеся обстоятельства не уменьшили интереса международного экспертного сообщества к поиску взаимоприемлемых решений по вопросам развития международного права, укрепления партнерства государства, бизнеса и гражданского общества для обеспечения международной информационной безопасности.

Позитивный потенциал наших дискуссий существенно вырос после образования здесь же в городе Гармиш-Партенкирхен в 2010 году Международного исследовательского консорциума. Сотрудничество заинтересованных организаций-членов Консорциума за прошедшее время позволило создать условия для объединения наших усилий в подготовке предложений по различным аспектам обеспечения международной информационной безопасности.

На предыдущей Десятой конференции Консорциума в г. Астане в ноябре прошлого года участники обменялись мнениями по некоторым актуальным научным проблемам обустройства киберпространства, выделили приоритетные темы дальнейших исследований, которые и составляют основу программы нашего Форума.

Завтра состоится организационное заседание одиннадцатой конференции Консорциума, на котором нам предстоит определиться с планами работы Консорциума на ближайшее будущее (время, место и тематика). Кроме того, состоится прием в организацию новых членов. Это:

Корпорация "ZTE" (Китайская Народная Республика);

Школа права Университета Корё (Республика Корея).

На обсуждение участников нашего Форума вынесены наиболее острые и неоднозначные вопросы формирования системы международной информационной безопасности, способной снизить опасность использования ИКТ для нарушения международного мира и безопасности.

Во-первых, предложения по механизмам адаптации международного права к киберпространству.

В рамках обсуждения данного вопроса на «круглом столе» предполагается обсудить:

- проблемы мирного разрешения киберконфликтов;
- международный правовой режим киберпространства, включая принципы международных отношений в киберпространстве, направления адаптации международного права конфликтов и международного гуманитарного права;
- механизмы объективизации данных о киберконфликтах и атрибуции субъектов кибератак;
- проблемы международного правового закрепления новаций в области международного права конфликтов и международного гуманитарного права применительно к киберпространству.

По поводу почти каждого из выделенных вопросов опубликовано значительное количество работ исследователей, представляющих разные научные школы, но искомое компромиссное решение так и не найдено.

Данное обстоятельство отчасти объясняется тем, что рассматриваемая проблема теперь уже связана не столько с отсутствием подходов к адаптации международного права к киберпространству, сколько с различием в подходах, предлагаемых специалистами разных стран. Так, международная группа специалистов, разработавших по заказу Центра кибербезопасности НАТО так называемое Таллиннское руководство, и специалисты этого же

Центра, подготовившие монографию по режиму мирного времени для деятельности государств в киберпространстве, предлагают, по существу, осуществлять адаптацию на основе доктринальных трактовок принципов международного обычного права. При этом, по-существу, они предлагают отказаться от некоторых наиболее важных, на наш взгляд, положений Устава ООН.

Например,

- изменить формулировку условий возникновения права государств на самооборону;
- размыть монополию Совета Безопасности ООН на легальное использование силы для обеспечения международного мира и безопасности;
- предоставить государствам право самостоятельно определять факты нарушения принципов и норм международного права, «назначать» виновное в этом государство и применять к нему контрмеры.

Кое-где в явном виде предлагается признать руководящую роль США в определении современного мирового порядка в киберпространстве, как государства, обладающего значительным киберпотенциалом.

Очевидно, что такой подход мы признать приемлемым не можем. Мы полагаем, что при всех обстоятельствах адаптация международного права должна сохранять основополагающую роль норм и принципов Устава ООН, а также укреплять центральное место Совета Безопасности ООН в механизме принятия решений о применении и реализации силы в международных отношениях.

Более подробно наши представления о контурах международного правового режима киберпространства будут обозначены в сообщениях на «круглом столе» №1.

Вторым важным направлением формирования системы международной информационной безопасности является реализация возможных инициатив по повышению информационной безопасности критически важных инфраструктур. Обсуждению этой проблемы будет посвящен «круглый стол» №2.

В рамках его работы предполагается рассмотреть вопросы:

- лучших практик в формировании систем информационной безопасности критически важных объектов;
- создания международных и национальных регламентов и стандартов обеспечения информационной безопасности критически важных объектов;
- формирования международной системы обеспечения информационной безопасности критически важных объектов;

• организации обмена информацией об инцидентах на критически важных объектах, взаимодействия CERT-ов в контексте выстраивания мер укрепления доверия.

Некоторые из выделенных вопросов уже длительное время являются предметом исследования ученых и специалистов. Другие — еще только начинают привлекать к себе внимание.

В данном контексте хотелось бы затронуть проблему идентификации объектов киберпространства, защищаемых международным гуманитарным правом. Очевидно, что без решения данной проблемы трудно рассчитывать на реальный успех в применении соответствующих норм международного гуманитарного права. Так, Приложение 1 к Дополнительному протоколу к Женевским конвенциям от 12 августа 1949 года полностью посвящено правилам, касающимся опознавания. Видимо, применение норм данного Протокола к условиям киберпространства также потребует отдельного приложения, посвященного правилам опознавания защищаемых объектов.

Сложной проблемой пока, как нам кажется, не имеющей приемлемого решения, является подготовка объективных юридически значимых документов по фактам нарушения норм международного права в киберпространстве. Мы надеемся, что в ходе работы «круглого стола» будут высказаны идеи, позволяющие объединить усилия всех заинтересованных сторон в данной области.

Третьей важной проблемой, вынесенной на обсуждение участников Форума, является обеспечение стабильности, устойчивости и безопасности сети Интернет. Некоторые юридические и технические аспекты данной проблемы будут обсуждены в рамках работы «круглого стола» №3. К числу запланированных тем отнесены следующие:

• политические, правовые, организационные и экономические проблемы обеспечения безопасности, устойчивости и стабильности инфраструктуры глобальной сети Интернет;

• технические стандарты и требования обеспечения безопасности, устойчивости и стабильности инфраструктуры глобальной сети Интернет;

• международные региональные и многосторонние правовые документы по проблемам безопасности, устойчивости и стабильности, а также правовые аспекты стандартизации.

Мы понимаем, что каждая из выделенных тем может стать предметом самостоятельного рассмотрения в будущем. Поэтому исходим из того, что на данном мероприятии будут выявлены их ключевые аспекты, которые являются наиболее сложными и заслуживают включения в программы следующих конференций.

Мы существенно перевыполним свои планы, если не ограничимся только выявлением этих ключевых аспектов, но и предложим взаимоприемлемые подходы к решению выявленных проблем.

Четвертой проблемой, вынесенной на обсуждение участников Форума, является противодействие угрозам вмешательства во внутренние дела суверенных государств через социальные медиа. Эта проблема будет обсуждаться на конференции впервые. В рамках «круглого стола» №4 предполагается затронуть вопросы:

- позитивных и негативных сторон социальных медиа как нового феномена общественной жизни;
- анализа и прогноза использования социальных медиа в деструктивных целях;
- механизмов противодействия угрозам вмешательства во внутренние дела суверенных государств на национальном и международном уровне.

Предложенные для обсуждения вопросы являются исключительно сложными, так как находятся на стыке международных обязательств государств по обеспечению прав человека в области свободы слова, самовыражения, а также функциональных задач государств по обеспечению национальной безопасности и поддержанию социальной стабильности. Мы знаем, что в этой области, как и в некоторых других областях обеспечения международной информационной безопасности, имеются существенные расхождения по позициям государств — членов ООН в области механизмов решения проблем в условиях разнонаправленных требований. Зачастую одно из этих разнонаправленных требований стремятся превратить в «Абсолют» в ущерб другому, а было бы лучше искать компромиссное решение. В связи с этим представляется важным найти пути налаживания открытого диалога, дискуссий, консультаций как на уровне международного экспертного сообщества, так и на уровне взаимодействия государств. Важно видеть проблему и стремиться к ее решению.

Наконец, еще одной проблемой, вынесенной на обсуждение участников Форума, является сравнение национальных приоритетов, а также подходов бизнеса (ИТ-индустрии) в области формирования системы международной информационной безопасности. По существу, в рамках «круглого стола» №5 будут анализироваться и сравниваться концептуальные представления экспертов о построении системы международной информационной безопасности, ее возможном облике, механизмах создания соответствующего правового, организационного, методического, кадрового и технического обеспечения.

Наш Форум проходит в период работы очередной Группы правительственных экспертов ООН по международной информационной безопасности (2014–2015 гг.), которой Генеральная ассамблея ООН поручила продолжить исследования по заданной тематике в рамках мандата. Представляется, что результаты наших дискуссий, высказанные здесь идеи в определённой мере будут использованы при подготовке итогового доклада Группы Генеральному Секретарю ООН, тем более, что некоторые участники заседания Группы присутствуют на нашем Форуме.

В заключение доклада хочу сообщить, что в работе конференции принимает участие около 80 ученых и специалистов из 13 государств мира (Россия, США, Канада, Великобритания, Германия, Швейцария, Италия, Австрия, Нидерланды, Эстония, Япония, Республика Корея, Киргизия), а также представители четырех международных организаций (МСЭ (Международный союз электросвязи), ОБСЕ (Организация по безопасности и сотрудничеству в Европе), ICANN (Международная корпорация по присвоению доменных имен и номеров), Консорциум военных академий и университетов «Партнерство ради мира»).

Подготовка и проведение такого представительного Форума были бы невозможны без помощи организаций-спонсоров. Я хотел бы перечислить наших партнеров-представителей этих организаций.

- Генеральный директор ФГУП «НТЦ «Атлас» Александр Николаевич Гридин;
- Научный руководитель НИИ автоматических систем РЖД Владимир Георгиевич Матюхин;
- Вице-президент корпорации ICAAN Вени Марковски.

Большой вклад в подготовку заседаний и содержательную проработку тематики «круглых столов» внесли наши партнеры-соорганизаторы заседаний:

- Международный комитет Красного Креста (круглый стол №1);
- Институт Восток-Запад (США) (круглый стол №2);
- Международная Корпорация Интернета по распределению адресов и номеров (ICANN) (круглый стол №3);
- Фонд SecDev (Канада) (круглый стол №4).

Огромное всем спасибо.

V.P.Sherstyuk

Co-Chairman of the Forum, Adviser of the Secretary of the Security Council of the Russian Federation, Director of Lomonosov Moscow State University Institute of Information Security Issues

Opening Remarks On Agenda and Challenges of the IX International Forum «Partnership of State Authorities, Civil Society and the Business Community in Ensuring International Information Security»

Dear participants of the conference!

Ladies and Gentlemen!

First and foremost, I would like to express my sincere gratitude to the people of Garmisch-Partenkirchen — thanks to their hospitality, experts in the field of information security from all over the world for the ninth year in a row can get together and discuss the most pressing issues of international peace and security in the context of increasing threat of misuse of information and communication technologies (ICT). These discussions will take place in an atmosphere of a certain aggravation of international relations and increase of political instability over the last year, which affected information space as well. These circumstances have not reduced the interest of the international expert community in finding mutually acceptable solutions to the issues of international law development, strengthening the partnership between the state, business and civil society to ensure international information security.

The positive potential of our discussions has significantly increased ever since International Information Security Research Consortium (IISRC) was established right here in Garmisch-Partenkirchen in 2010. The cooperation between the interested organization-members of the Consortium played a role in forming of the environment necessary to bring together our efforts in the preparation of proposals on various aspects of international information security.

In the course of the previous, tenth IISRC conference in Astana in November last year, the participants exchanged views on some challenging scientific issues of development of cyberspace and identified

priority topics for further research, which form the basis of the agenda of our Forum.

Tomorrow there will be an organizational meeting of the Eleventh conference of the Consortium, where we will decide on the work plans of the Consortium for the near future (time, place and subject matter). Also, new members will be admitted to the organization: ZTE Corp. (China); Cyber Law Centre of Korea University (Republic of Korea).

The most pressing and controversial issues of development of international information security system are brought up to discussion by participants of our Forum. This system can reduce the risk of the use of ICTs for violation of international peace and security.

Firstly, proposals on the Frameworks for Adaptation of International Law to Conflicts in Cyberspace. The discussion at the round table is expected to touch upon the following questions:

- Challenges of peaceful resolution of cyberconflicts;
- Principal directions of International Humanitarian Law adaptation to cyberspace;
- Frameworks of cyberconflicts data objectification and attribution of subjects of cyberattacks;
- Challenges of international-legal legitimization of International Humanitarian Law developments with regard to cyberspace.

There is a considerable amount of research papers on almost all of the mentioned issues published by representatives of various schools of thought, but the desired solution has not yet been found.

This is partly due to the fact that currently this issue is associated not so much with the lack of approaches to adaptation of international law to cyberspace, but with the differences of approaches offered by specialists from different countries. Specifically, an international group of experts, which developed a so-called Tallinn manual at request of NATO Cooperative Cyber Defence Centre of Excellence, and experts of this Center, which have published a monograph on a peacetime regime for activities of nation-states in cyberspace, essentially offer to carry out adaptation on the basis of doctrinal interpretations of the principles of the customary international law. At that they ultimately offer to give up some of the most important, in our opinion, provisions of the UN Charter.

For example,

- to change description of the conditions of accrual of the right to self-defense;

- to degrade the monopoly of the UN Security Council on the legal use of force for safeguarding of international peace and security;
- to give nation-states the right to determine by themselves violations of the principles and norms of international law, «appoint» the responsible countries and apply countermeasures.

In parts there are proposals in an explicit form to recognize the leading role of the United States in determining the contemporary global order in cyberspace, as they have significant cyber capabilities.

Obviously, we cannot recognize this approach as acceptable. We believe that in all circumstances the adaptation of international law must preserve the fundamental role of the norms and principles of the UN Charter, as well as strengthen the pivotal role of the UN Security Council in decision-making framework for application and implementation of force in international relations.

Our vision about the contours of international legal regime in cyberspace will be specified in greater detail in the reports in the course of the Workshop — Round table 1.

The second important area of development of the international information security system is implementation of possible initiatives to improve the security of critical information infrastructures. Workshop — Round table 2 will be dedicated to the discussion of this issue. It is planned to consider the following issues:

- National best practices of development of Critical Infrastructure (CI) Information Security;
- Challenges of development of International and national regulations and standards of CI Information Security;
- Development of an international system of Critical Infrastructure (CI) Information Security;
- Challenges of international Data sharing on CI cyber incidents and issues of CERTs cooperation with regard to confidence building measures.

Some of the highlighted issues have long been a subject of work of researchers and experts, while the others are just beginning to draw attention.

In this context I would like to touch upon the issue of identification of objects in cyberspace that are protected under international humanitarian law. It is obvious that without a solution to this problem we can hardly expect a real success in application of the relevant norms of international humanitarian law. For example, Annex 1 of the Additional Protocol to the Geneva Conventions of 12 August 1949 is

entirely dedicated to the rules of identification. Apparently the application of the Protocol to cyberspace will also require a separate Annex, concerning the rules of identification of the protected objects.

It seems that preparation of objective documentation about facts of international law violations in cyberspace, remains a challenging problem that has no acceptable solution. As we hope, some ideas that could bring together all relevant stakeholders will be expressed in the course of a Workshop — Round table.

The third important issue to be discussed at the Forum is ensuring Stability, Reliability and Security of the Internet. Some legal and technical aspects of the issue will be discussed in the course of the Workshop — Round table 3. Planned topics for the discussion include the following:

- Challenges (political, legal, institutional and economical) of ensuring safety, integrity and reliability of Internet Infrastructure;
- Technical standards and specifications of ensuring safety, integrity and reliability of Internet Infrastructure;
- International regional and multilateral legal documents relevant to safety, integrity and reliability and legal aspects of technical standardization;

As we see it, each of these issues can become a subject of an independent research in the future. Therefore we presume that this event will identify their crucial, most complex aspects, worthy to be put on the agenda of the following conferences. We will significantly exceed our plans, if we will not only identify the key aspects, but also offer mutually acceptable solutions to the relevant issues.

The fourth problem to be discussed at the Forum is countering of the threat of the use of social media for interference in the internal affairs of sovereign states. This issue will be discussed at the conference for the first time. The following issues will be discussed as part of the Workshop — Round table 4:

- Social media as a new phenomenon of public life: benefits and implications;
- Use of Social media for destructive purposes: analysis and prognosis;
- International and national mechanisms of countering the threat of interference in the internal affairs of sovereign states.

The topics proposed for the discussion are extremely complex, since they are at the junction of international obligations of nation-states to ensure the rights of freedom of speech and expression, and functional tasks of national security and maintaining of social stability. We know

that in this area, as in some other areas of international information security, there are significant differences between the positions of the United Nations member states considering the frameworks for solving problems under competing requirements. It is not uncommon that one of these competing requirements is turned into «Absolute» to the detriment of another, and it would be better to seek a compromise solution. In this regard, it is important to find paths to an open dialogue, discussions and consultations at the level of international expert community, and at the level of state-to-state interaction. It is important to recognize a problem and try to solve it.

Finally, yet another issue to be discussed at the Forum, is comparison of National Priorities and Business Approaches (IT-industry) in the sphere of International Information Security System Development. In essence, Workshop — Round table 5 will be dedicated to analysis and comparison of conceptual views of experts on the development of international information security system: its possible conceptual structure, frameworks for the development of appropriate legal, organizational, methodological, staffing and technical support.

Our conference is held as the new UN Group of Governmental Experts on international information security (2014–2015) continues its work with the mandate of the UN General Assembly to further the research in this area. It seems that to a certain extent the outcome of our discussion may be used in preparation of the final report to the UN Secretary General; moreover several members of the Group are present at our Forum.

In conclusion I would like to mention that among the participants of the Forum there are over 80 scientists and experts from 13 countries of the world (the Russian Federation, the USA, Canada, the United Kingdom, Germany, Switzerland, Italy, Austria, the Netherlands, Estonia, Japan, Republic of Korea, Kyrgyzstan), as well as the representatives of four international organizations (ITU (International Telecommunication Union), OSCE (Organization for Security and Cooperation in Europe), ICANN (International Corporation for Assigned Names and Numbers), Consortium of defence academies and security studies institutes, «Partnership for Peace»).

It would have been impossible to prepare and carry out such a representative Forum without the assistance of the sponsoring organizations. I would like to mention our partners-representatives of these organizations.

- General Director of FSUE “STC Atlas”Alexander Gridin;

- Supervisor of the Research Institute of automated systems, Russian Railways Vladimir G. Matyukhin;
- Vice-president of ICAAN Veni Markovski.

Our partners and co-organizers have made a great contribution to preparation of meetings and scientific elaboration of the round-tables:

- The International Committee of the Red Cross (round-table №1);
- East-West Institute (USA) (round-table №2);
- International Internet Corporation for Assigned Names and Numbers (ICANN) (round-table №3);
- SecDev Foundation (Canada) (round-table №4).

Thank you all very much.

С.М.Буравлев

Сопредседатель оргкомитета Форума,
заместитель Секретаря Совета Безопасности Российской Федерации

Приветствие к организаторам, участникам и гостям IX международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности»

Уважаемые коллеги!

Позвольте приветствовать организаторов, участников и гостей международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности».

Стало доброй традицией ежегодно в апреле собирать на баварской земле ведущих специалистов, занимающихся проблемами обеспечения информационной безопасности. В девятый раз представители государственных структур, известные ученые и эксперты научных и образовательных центров из 13 стран мира примут участие в работе Форума. В этом году на встрече продолжится дискуссия по ключевым вопросам в наиболее чувствительной на сегодняшний день сфере обеспечения безопасности.

Очевидно, что обеспечение безопасности государства, общества и личности в информационной сфере в условиях нарастания новых вызовов и угроз с учетом их трансграничного характера возможно только на основе качественно новых, научно обоснованных подходов и решений.

При этом необходимость противодействия возрастающей опасности деструктивных информационных воздействий в глобальном информационном пространстве требует консолидации усилий государств, научного и экспертного сообщества, бизнес-структур и гражданского общества. Необходим поиск путей формирования эффективной системы обеспечения международной информационной безопасности.

Форум в Гармиш-Партенкирхене является уникальной площадкой, где ученые и эксперты могут обсуждать ключевые проблемы в области информационной безопасности и предлагать максимально выверенные пути их решения.

Традиционно повестка дня Форума ориентирована на обсуждение актуальных задач обеспечения безопасности в информационной сфере. Сегодня одной из самых дискуссионных тем в рассматриваемой области стала применимость международного права к деятельности государств в информационном пространстве, к сфере использования информационных и коммуникационных технологий в целом.

Поэтому закономерно, что данная тема в этом году открывает диалог участников Форума, в рамках которого будут обсуждаться актуальные и наиболее значимые правовые вопросы обеспечения международной информационной безопасности. Уверен, что представители научного и экспертного сообщества не только обсудят проблемы в данной области, но и предложат перспективные направления международно-правового регулирования межгосударственных отношений в глобальном информационном пространстве.

Безусловно, для обеспечения информационной безопасности необходим не только международно-правовой фундамент, но и сформированные на его основе системные решения наиболее острых проблем. Среди них — повышение защищенности критически важных инфраструктур, обеспечение стабильного, безопасного и устойчивого функционирования сети Интернет, а также противодействие угрозам использования информационных и коммуникационных технологий для вмешательства во внутренние дела суверенных государств.

В этой связи итогом встречи в Гармиш-Партенкирхене должно стать определение приоритетных направлений совершенствования системы международной информационной безопасности.

Желаю успешной и плодотворной работы!

S.M.Buravlev

Co-Chairman of the Forum, Deputy Secretary of the Security Council of the Russian Federation

Welcome Address to the organizers, participants and guests of the IX International Forum «Partnership of State Authorities, Civil Society and the Business Community in Ensuring International Information Security»

Dear colleagues!

Allow me to welcome the organizers, participants and guests of the International forum «Partnership of State Authorities, Civil Society and the Business Community in Ensuring International Information Security».

It has become a good yearly tradition for the leading information security experts to gather on Bavarian soil in April. For the ninth time the representatives of the governments, renowned scientists and experts from scientific and educational centers of 13 countries of the world will take part in the Forum. This year's meeting will further the discussion of the key issues in the most delicate sphere of security.

It is evident that in the context of new threats and challenges with regard to their cross-border nature, it is possible to maintain security of the nation-state, society and individuals in the information sphere only on the basis of breakthrough science-based approaches and solutions.

At the same time the need to counter the growing threat of destructive information impacts in the global information space requires the consolidation of efforts of the nation-states, scientific and expert community, business and civil society. We need to find the lines of approach to development of an effective international information security system.

Forum in Garmisch-Partenkirchen is a unique platform where scientists and experts can discuss the key issues in the field of information security and offer the most balanced solutions.

The agenda of the Forum is traditionally focused on the discussion of the challenging problems of security in the information sphere. Today one of the most controversial topics in this area is applicability of international law to activities of nation-states in information space, and to the sphere of information and communication technologies in general.

Therefore naturally this topic will open up a dialog between the participants of this Forum which will consider topical and most significant legal issues of international information security. I am confident that the representatives of scientific and expert community will not only discuss issues in this area, but also offer promising directions for international legal regulation of interstate relations in the global information space.

Undoubtedly, maintaining of information security requires not only international legal foundations, but also solutions to the most pressing problems, based on these foundations. Among them — improving the security of critical infrastructures, ensuring a stable, secure and resilient functioning of the Internet, as well as countering the threat of ICTs use for interference in the internal affairs of sovereign states.

In this regard, the meeting in Garmisch-Partenkirchen should identify and elaborate the focal areas for development of international information security system.

I wish you successful and fruitful work!

А.В.Соколов

Заместитель министра, Министерство связи и массовых коммуникаций Российской Федерации

Выступление на XI международном форуме «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности»

Инновационное развитие телекоммуникационных технологий, глобальный и открытый характер Интернета уже стали устойчивым трендом развития в 21 веке, а обеспечение гарантированного свободного доступа граждан к информации — одной из основополагающих задач государства. Мы даже можем говорить о новой формации общественного развития, когда информационное общество переходит в общество знаний, а информация и знания не только доступны технически, но и неразрывно связаны с развитием личности.

Интернет-среда должна быть устойчивой к внешним воздействиям и необходимость усиления внимания всех государств к проблеме управления интернетом является очевидной.

Главные направления действий России — это создание условий, при которых граждане Российской Федерации, где бы они ни жили, имели возможность равного доступа к информации, современным услугам связи, имели возможность получения государственных услуг онлайн.

Россия прилагает значительные усилия по развитию инфраструктуры широкополосного доступа для жителей небольших и удаленных населенных пунктов, в 2018 году уровень проникновения услуг ШПД должен будет достичь 97%.

Мы продолжаем работу по переводу государственных органов на электронный документооборот, и обеспечению дистанционного доступа к государственным услугам. Интернет становится средой для выстраивания отношений между гражданами и государством. Очевидно, что мы хотим, чтобы эта среда была безопасной, стабильной и предсказуемой.

Россия исходит из понимания того, что Интернет должен оставаться открытым, не фрагментированным глобальным ресурсом, наделенным справедливым и по-настоящему международным механизмом управления.

Важно вспомнить, что данный форум происходит в преддверии Всемирной встречи на высшем уровне по вопросам информационного общества, которая состоится в конце 2015 года.

Российская Федерация, как и многие другие страны, последовательно выступает за продолжение данного процесса и принятие соответствующего решения на Генеральной Ассамблее ООН.

Объективная реальность показывает, что не все задачи, поставленные 10 лет назад, реализованы, возникли и новые вызовы. Разрыв в цифровых технологиях не ликвидирован. Мы все больше сталкиваемся с проблемами информационной безопасности, защиты права на неприкосновенность частной жизни при использовании Интернета. Постоянно совершенствуются способы противоправной деятельности в информационной среде, в том числе и на трансграничной основе. Значительные доходы приносят такие виды преступлений как кибератаки на ресурсы частных и, особенно, финансовых структур, мошенничество с банковскими карточками, воровство персональных данных граждан и так далее.

Отдельно выделяем вопрос защиты персональных данных граждан. Поддерживаем принцип ответственности глобальных интернет-компаний в отношении сбора, анализа и хранения персональных данных и право человека самостоятельно управлять личным пространством в сети, исключающим навязывание информации и влияние на его информационное поле.

Мир меняется и нам нужно адаптироваться к новым вызовам. Информационные технологии должны стать одним из ключевых факторов поступательного экономического роста и развития человечества, помочь выровнять возможности развитых и развивающихся стран, раскрыть профессиональные и творческие способности человека.

Для успешного, надёжного и безопасного использования информационных технологий, необходимы международные нормы и правила, регулирующие отношения в этой области.

Россия полагает, что такие нормы должны вырабатываться под эгидой институтов ООН. Они должны исходить из приверженности принципам невмешательства во внутренние дела государств, их равноправия в процессе управления Интернетом, быть основаны на международном праве и соблюдении основных прав и свобод человека и учитывать накопленный за годы развития Интернета опыт нахождения консенсуса участниками сети по различным вопросам.

Сегодня Интернет проникает во все сферы личной и профессиональной жизни людей, не только открывая новые возможности, но и делая мир всё более уязвимым. Любой значительный сетевой сбой может привести к экономическому и социальному коллапсу. Интернет-среда должна быть устойчивой ко внешним негативным воздействиям.

Исходя из того, как устроен Интернет, мы видим потенциальные уязвимости в работе системы доменных имён, возможны искажение информации в базе данных регистратур, приводящая к невозможности проверки маршрутно-адресной информации и построения верных маршрутов трафика в сети Интернет.

Разумеется, они не новы и, насколько нам известно, изучаются и в других странах. Устранять их нужно на межгосударственном уровне, на основе согласованных всеми «правил поведения» в информационном пространстве.

Необходимо равноправное участие государств в управлении Интернетом, в обеспечении открытого, гарантированного и безопасного доступа к услугам информационный технологий для всех жителей мира.

В конце хочу отметить и подчеркнуть готовность России обсуждать различные идеи и предложения, мы стремимся внести свой собственный вклад и на своей территории обеспечить бесперебойное функционирование сети Интернет, свободный доступ к ее ресурсам и их защиту.

Желаю всем участникам успешной работы и новых конструктивных решений и идей!

Благодарю за внимание!

A.V.Sokolov

Deputy Minister, Ministry of Telecom and Mass Communications of the Russian Federation

Address at the IX International Forum «Partnership of State Authorities, Civil Society and the Business Community in Ensuring International Information Security»

Innovative development of telecommunication technologies, the global and open nature of the Internet have become a stable trend of development in the 21st century, and provision of guaranteed free access to information — has become one of the fundamental tasks of the nation-state. One may even talk of a new type of social development when an information society becomes a knowledge society and information and knowledge are not only technically available, but also are inextricably linked with the development of the individual.

Internet environment must be resilient to external effects, and there is an obvious need to focus the attention of all nation-states to the issue of Internet governance.

The main direction of actions of leadership in Russia — is to create conditions under which Russian citizens, wherever they live, would have available an equal access to information and modern communication services, would have the possibility to use the governmental services online.

Russia puts out considerable efforts for the development of broadband infrastructure in small and remote communities; by 2018 broadband penetration is expected to reach 97%.

We continue to work on the transition of government agencies to an electronic document management, and enabling remote access to government services. The Internet becomes a medium for building relations between the citizens and the nation-state. Obviously, we want this environment to be secure, stable and predictable.

Russia proceeds from the understanding that the Internet should remain open, and not fragmented global resource, equipped with fair and truly international control framework.

It is important to remember that this Forum takes place on the eve of the World Summit on the Information Society, to be held at the end of 2015.

The Russian Federation, as well as many other countries, has consistently advocated the continuation of this process and adoption of the relevant decision in a session of the UN General Assembly.

Objective reality shows that not all goals, which were set 10 years ago, have been implemented, and new challenges have emerged. The digital divide has not been eliminated. We face the increasing problems of information security, and ensuring of privacy when using the Internet. Methods of illegal activities in the information environment, including transnational ones, are constantly developing. Significant profit is generated by such crimes as cyberattacks on resources of private and especially financial institutions, bank card fraud, theft of citizens' personal data, and so on.

We place special emphasis on the issue of personal data protection. We support the principle of the responsibility of the global Internet companies concerning collection, analysis and storage of personal data and the right of an individual to manage personal space on the network in such a way as to avoid the imposition of information and the impact on his information field.

The world is changing and we need to adapt to the new challenges. Information technologies must become one of the key factors of onward economic growth and human development, help equalize the capabilities of the developed and developing countries and reveal professional and creative capabilities of mankind.

Successful, reliable and secure use of information technology requires international norms and rules for regulating the relations in this field.

Russia believes that such rules should be developed under the auspices of the UN institutions. They should be based on adherence to the principles of non-interference in the internal affairs of nation-states and their equality in the process of Internet governance, be based on international law and observance of fundamental human rights and freedoms and to take into account the experience of consensus-building on various issues accumulated by the participants of the network over the years of development of the Internet.

Today the Internet enters all aspects of personal and professional life of individuals and opens up new opportunities, but also makes the world more and more vulnerable. Any significant network failure could lead to economic and social collapse. Internet environment must be resilient to external negative influences.

Taking into consideration the design of the Internet, we see potential vulnerabilities in the Domain Name System, where there is a possibility of distortion of information in the database registries, which would make impossible the verification of route-address information and correct routing on the Internet.

Of course these vulnerabilities are not new and, as far as we know, are looked into by other countries. Vulnerabilities should be addressed at the international level, on the basis of consensual «rules of conduct» in the information space.

There is a need in equitable participation of the nation-states in Internet governance and provision of an open, secure and safe access to information technology for all people in the world.

Lastly, I would like to note and emphasize that Russia is ready to discuss various ideas and suggestions; we are committed to making our own contribution and ensure on our territory the smooth functioning of the Internet, free access to its resources and their protection.

I wish all the participants successful work and new constructive solutions and ideas! Thank you for your attention.

И.Н.Дылевский, С.А.Комов
Министерство обороны Российской Федерации

Правила поведения в информационном пространстве — альтернатива гонке информационных вооружений»

Уважаемые коллеги!

Современные информационные технологии все чаще используются в агрессивных целях. В сочетании с экстремистскими, националистическими, расистскими действиями они способны дестабилизировать обстановку и устранить от власти любое правительство как в самом развитом, так и в отсталом государстве.

Сегодня ни одна страна мира не может считать себя защищенной от трансграничных информационных угроз.

Информационные технологии могут стать детонатором развязывания даже межгосударственного **военного конфликта.**

Причем для создания конфликтной ситуации требуется гораздо меньше затрат чем классическая подготовка традиционной войны. При этом не нужно создавать крупных группировок войск, концентрировать в определенных районах авиацию, артиллерию, противовоздушную оборону, подтягивать логистические подразделения и так далее.

Информационные воздействия являются бескровными, не разрушают окружающую среду и могут реализовываться через вполне мирные средства — СМИ, «Интернет», средства телекоммуникаций, информатики, связи и др.

Посредством дезинформационных вбросов, публикаций и распространения экстремистских заявлений, проведения расистских или ксенофобских флэшмобов, трансграничных компьютерных атак на критически важные для жизни и деятельности общества объекты и т.п. возможно «разогреть» ситуацию в любой стране до «социального взрыва».

Подобными действиями также можно поссорить несколько государств и довести их до состояния войны.

На примерах цветных революций и конфликтов последнего десятилетия можно с уверенностью сказать, что такие технологии уже достаточно хорошо обкатаны.

Вопрос: где, когда и против кого они будут применены в дальнейшем?

Еще один вопрос: какое государство сегодня с полной уверенностью сможет однозначно ответить — против него эти технологии применить не возможно, потому, что оно полностью защищено?

Ответ очевиден — таких государств не существует.

Еще одним аспектом борьбы в информационной сфере является быстро совершенствующееся и распространяющееся **информационное оружие.**

Экспертами не раз уже отмечалось, что ущерб от его использования может приводить к техногенным катастрофам на критически важных объектах промышленности, экономики, энергетики и транспорта, к финансовому коллапсу и системному экономическому кризису.

С развитием информационных технологий будет расширяться линейка информационного оружия, а также увеличиваться перечень объектов, по которым возможно его применение.

Ситуацию обостряет тот факт, что данное оружие может попасть в руки террористов и криминальных структур. В этом случае последствия его применения будут не предсказуемы.

Многие эксперты сходятся во мнении, что запретить разработку такого оружия, а главное проконтролировать его наличие у государств, а тем более террористов нельзя.

Но выработать механизм его нераспространения возможно.

Сегодня многим государствам стало очевидным, что пора принять универсальные правила, которые будут способствовать предотвращению использования информационных технологий для развязывания войн и вооруженных конфликтов.

Например, в январе этого года такую инициативу предпринята Шанхайская организация сотрудничества, внеся в ООН проект искомых правил поведения[1].

Государства, входящие в ШОС, предлагают принять членам мирового сообщества обязательства не использовать ИКТ в целях, противоречащих поддержанию международного мира и безопасности, укреплять доверие и воздерживаться от применения силы или угрозы силой в информационном пространстве.

К сожалению, некоторые страны считают иначе. По их представлениям, для поддержания мира и безопасности в информационном пространстве нужно придерживаться стратегии устрашения.

Действительно, в годы «холодной войны» взаимная угроза ядерного возмездия позволила избежать развязывания крупно-

---

[1] Правила поведения в области обеспечения международной информационной безопасности, Документ ООН А/69/723/, 13 января 2015.

масштабной войны. Однако это еще не повод для того, чтобы только на основе устрашения пытаться предотвращать конфликты, которые, как полагают на Западе, могут возникнуть в результате применения информационного оружия[2].

Считаем, что такой подход несет серьезную угрозу международной безопасности, так как он основывается на создании и демонстрации мощного военного информационного потенциала. Этот шаг неизбежно приведет к гонке информационных вооружений, грубому нарушению принципа равной безопасности и общей дестабилизации военно-политической обстановки в мире.

Кроме того, российские военные эксперты полагают, что сравнение нынешнего исторического периода с ситуацией начала «холодной войны» не корректно.

Оценивая высказывания главы американского киберкомандования М. Роджерса, что «обретение США ядерной мощи ... позволило снизить конфронтацию и в итоге привело к переговорам по контролю над вооружениями»[3], считаем — все было с точностью наоборот. Именно создание ядерного потенциала СССР привело к балансу сил и позволило избежать катастрофы развязывания ядерной войны, а в конечном итоге вынудило США пойти на те самые переговоры.

Что касается современной ситуации, то хочу заострить ваше внимание на следующем.

Сегодня нет «холодной войны». Поэтому такие заявления М.Роджерса, как «...наши противники полны решимости контролировать свои сегменты киберпространства, красть нашу интеллектуальную собственность и дезорганизовывать работу наших ведомств» и «...у нас мало надежды, что они будут вести себя ответственно в киберпространстве» вызывают недоумение.

Пока мы наблюдали обратную картину. По свидетельствам Э.Сноудэна, США в информационном пространстве шпионят не только за противниками, но и за союзниками, и за собственными гражданами.

---

[2] Дж. Най Геополитика сдерживания кибератак между государствами в Интернете, http://kiber.akipress.org/news:192; К.Гирс Сдерживание информационного противоборства, http://www.iisi.msu.ru/forum/stenogramma/; Statement of Admiral Michael S Rogers Commander United States Cyber Command before the Senate Committee on Armed Services, 19 March 2015, http://www.armed-services.senate.gov/imo/media/doc/Rogers_03-19-15.pdf

[3] Statement of Admiral Michael S Rogers Commander United States Cyber Command before the Senate Committee on Armed Services, 19 March 2015, http://www.armed-services.senate.gov/imo/media/doc/Rogers_03-19-15.pdf

Поэтому нам не понятны мотивы, побуждающие Соединенные Штаты опираться не на силу права, а на право силы, основанное на реализации стратегии устрашения в информационном пространстве.

Теперь мне бы хотелось высказаться на данную тему в содержательном ключе. Скажу сразу, что мы отрицательно относимся к самой идее «информационного устрашения» и скептически к ее реализуемости.

Во-первых, в отличие от ядерного оружия при применении информационных технологий не существует явной угрозы взаимного гарантированного уничтожения. Следовательно, у политического руководства сторон конфликта не будет того страха развязывания «информационной войны», который эффективно мотивирует реальность ядерного возмездия.

Во-вторых, учитывая большое количество негосударственных акторов, действующих в информационном пространстве, представляется некорректным использовать аналогию с ядерным устрашением, которое, по сути, было реализовано двумя основными ядерными державами — СССР и США. Сейчас может оказаться недостаточно одному из двух государств, обладающих сопоставимыми информационными потенциалами, убедить другое не идти на эскалацию конфликта для того, чтобы предотвратить его перехода в горячую стадию.

В-третьих, образцы информационного оружия значительно легче разработать, произвести и передать кому-бы то ни было, чем технологии ядерного оружия. Поэтому достичь убедительного превосходства над соперниками чрезвычайно трудно.

В-четвертых, источник информационной атаки в компьютерных сетях сложно установить ввиду его анонимности и комплекса специальных мер, принимаемых для «запутывания» следов. Поэтому оперативно расследовать произошедший инцидент и достоверно собрать все необходимые доказательства для совершения легитимного «акта возмездия», который будет оправдан мировым сообществом, вряд ли получится.

В-пятых, мы полагаем, что в информационном пространстве будет весьма затруднительно обеспечить баланс военных информационных потенциалов на основе достоверного знания основных характеристик системы информационного вооружения сторон.

С одной стороны, публикация сведений о разработке новых систем вооружения немедленно приведет к разработке средств и способов противодействия им, т.е. к нарушению баланса. С другой стороны, любая неконтролируемая скрытая разработка таких

систем также будет нарушать искомый баланс, и дестабилизировать военно-политическую обстановку.

Хочу заметить, что пока известен единственный исторический пример, демонстрирующий мощь информационного оружия. Это атака компьютерного вируса Stuxnet на иранские ядерные объекты в Натанзе и Бушере. Можно предположить, что она замышлялась как реинкарнация ядерных бомбардировок Хиросимы и Нагасаки. Однако в результате этой атаки мир не содрогнулся, а Иран не объявил о своей капитуляции и отказе от ядерных программ. Значит, потенциал информационных вооружений пока не сопоставим с мощью ядерного оружия, а ставка на его дальнейшее наращивание в принципе ошибочна.

Если государства возьмут курс на информационное устрашение, то это приведет лишь к новому витку гонки вооружений и милитаризации информационного пространства.

Единственной разумной альтернативой этому безумию является упомянутая мирная инициатива в области международной информационной безопасности, продвигаемая в ООН государствами ШОС.

Она также направлена на предотвращение информационной агрессии. Однако в отличие от стратегии устрашения основывается не на страхе возмездия, а на добровольном принятии универсальных правил поведения государств в информационном пространстве, добросовестное выполнение которых обеспечит мир, стабильность и равную безопасность всем народам в глобальном информационном пространстве.

Мы выступаем за широкое международное сотрудничество в решении глобальной проблемы противодействия угрозе развязывания информационных войн, распространения информационного оружия. При этом основной целью развития сотрудничества, по нашему мнению, является установление международно-правового режима обеспечения международной информационной безопасности, регулирующего, в том числе, военную деятельность государств в мировом информационном пространстве на основе принципов и норм международного права. Мы выступаем за создание механизмов двустороннего и многостороннего сотрудничества по военным аспектам международной информационной безопасности.

Благодарю за внимание!

I.N.Dylevsky, S.A.Komov
Ministry of Defense of the Russian Federation

Rules of conduct in information space – an alternative to an information arms race

Dear Colleagues!

Contemporary information technologies are increasingly being used for aggressive purposes. Combined with extremist, nationalist, racist actions, they are able to destabilize the situation and remove any government from power both in the most developed and undeveloped country alike.

Today no country can consider itself secure from the cross-border information threats.

Information technologies can become a trigger for unleashing even an interstate **armed conflict**.

At that, much lower expenses are required to create a conflict situation in comparison with the classical preparation of conventional war. You do not need to create large groupings of forces, concentrate aviation, artillery, air defense in certain areas, and bring up logistics divisions and so on.

Information influence is without bloodshed, does not destroy the environment and may be implemented through quite peaceful means — mass media, the Internet, means of telecommunications, computer and communications capabilities and etc.

Through actions of misinformation, publication and dissemination of extremist statements, gathering of racist or xenophobic flash-mobs, cross-border cyberattacks on objects critical to daily living activities of society, etc. the situation in any country can be «brought to the boil» and lead to «social upheaval».

Such actions can also be used to put several States at odds with each other, and to bring them to a state of war.

Drawing on the example of color revolutions and conflicts of the last decade one can say with confidence that such technologies have already been well run in.

The question is where, when and against whom will they be applied in the future?

Another question is what nation-state today can unequivocally and with confidence say that it is impossible to use these technologies against it, because it is fully protected?

The answer is obvious — there is no such nation-state.

Another aspect of confrontation in the information sphere is a rapid advancement and proliferation of **information weapons**.

Experts have repeatedly noted that the damage caused by the use of such weapons may lead to industrial disasters on critical facilities of industry, economy, energy production and transport, collapse of financial system and economic crisis.

With the development of information technologies the range of information weapons will expand, and the list of objects that can become targets for its possible use will extend.

The situation is exacerbated by the fact that such weapons could fall into the hands of terrorists and criminal organizations. In this case its effects will be unpredictable.

Many experts share the view that it is impossible to prohibit the development of such weapons, and most importantly to monitor its on-hand status in nation-states, let alone terrorist groups.

But it is possible to develop a framework for their non-proliferation.

Today, it has become apparent for many nation-states that it is time to adopt universal rules that will help prevent the use of information technology to unleash wars and armed conflicts.

For example, in January of this year, the Shanghai Cooperation Organization undertook such initiative, and submitted to the United Nations a draft of a sought-for code of conduct[1].

The SCO member-states propose the international community to adopt the obligations not to use ICTs in a manner contrary to maintenance of international peace and security, to build confidence and to refrain from threat or use of force in information space.

Unfortunately, some countries believe otherwise. In their view, to maintain peace and security in information space one must adhere to the strategy of deterrence.

Indeed, in the years of «cold war» the mutual threat of nuclear retaliation allowed us to escape the unleashing of a large-scale war. However, that cannot be a reason to try to prevent conflicts only on a basis of deterrence — conflicts that, as believed in the West, may result from the use of information weapons[2].

---

[1] International code of conduct for information security, UN Document A/69/723/, January, 13 2015.

[2] J.Nye The Mouse Click that roared, http://www.project-syndicate.org/commentary/addressing-the-cyber-security-challenge-by-joseph-s--nye; K.Geers Deterrence of Cyber Warfare, http://www.iisi.msu.ru/forum/stenogramma/; Statement of Admiral Michael S Rogers Commander United States Cyber Command before the Senate Committee on Armed Services, 19 March 2015, http://www.armed-services.senate.gov/imo/media/doc/Rogers_03-19-15.pdf

We believe that this approach poses a serious threat to international security, since it is based on building and display of powerful military information capabilities. This move will inevitably lead to an information arms race, a serious violation of the principle of equal security and general destabilization of the military-political situation in the world.

Moreover, Russian military experts believe that the comparison of the current historical period with the situation in the beginning of the «cold war» is inappropriate.

Evaluating the statement of the head of the US Cyber Command Michael S. Rogers that «the acquisition of a nuclear potential by the US... made it possible to reduce confrontation and eventually led to negotiations on arms control», we think that the situation was exactly the opposite. The creation of a nuclear potential of the USSR was the event that led to a balance of power and allowed to avoid the catastrophe of a nuclear war, and ultimately forced the US to enter the very same negotiations.

With regard to the current situation, I would like to draw your attention to the following.

Today there is no «cold war». Therefore, such statements by Michael S. Rogers as «...our opponents are determined to control their segments of cyberspace, steal our intellectual property, and disrupt the work of our institutions» and «...we have little hope they will behave responsibly in cyberspace» leave us perplexed.

Meanwhile, we have observed a different picture. According to the testimony of Edward Snowden, the United States are spying not only after adversaries but also allies and their own citizens in information space.

Therefore, we do not understand the motives which determine that the United States rely not on the force of law but the rule of force, based on the implementation of a deterrence strategy in information space.

Now I would like to elaborate on this subject in an insightful way. I have to say that we have a negative attitude towards the very idea of «information deterrence» and are skeptical about its feasibility.

Firstly, unlike nuclear weapons, the use of information technologies doesn't give raise to imminent threat of mutually assured destruction. Consequently, the political leadership of the parties to the conflict will not have the same fear of unleashing an «information war», which effectively motivates the reality of nuclear retaliation.

Secondly, given the large number of non-state actors operating in information space, it seems incorrect to use the analogy of nuclear deterrence, which in fact has been implemented by two major nuclear

powers — the USSR and the USA. Now in order to prevent the transition of a conflict to the «shooting stage» it may be insufficient for one of the two nation-states with comparable information capabilities to convince the other not to escalate the conflict.

Thirdly, information weapons are much easier to develop, produce and transfer to someone else than military nuclear technologies. Therefore, it is extremely difficult to achieve a convincing superiority over the competitors.

Fourthly, is difficult to attribute the source of information attack on computer networks because of its anonymity and a set of special measures taken for «double backing» of traces. Therefore, it is unlikely to promptly investigate the incident and reliably collect all the necessary evidence for legitimate «retaliation», which will be justified by the international community.

Fifthly, we believe that in information space it will be very difficult to achieve a balance of military information capabilities based on reliable knowledge of key parameters of information weapons of the parties.

On the one hand, publication of information on development of new weapons systems will immediately result in development of tools and methods to counter them, i.e. disrupt the balance. On the other hand, any uncontrolled and covert development of these systems will also disrupt the balance, and destabilize the military and political situation.

I would like to note that for the time being there is only one known historical example that demonstrates the power of information warfare. It is the attack of Stuxnet computer virus on Iran's nuclear facilities at Natanz and Bushehr. It can be assumed that it was conceived as a reincarnation of the nuclear bombings of Hiroshima and Nagasaki. However, the world has not trembled as a result of this attack, and Iran has not announced its surrender and the abandonment of nuclear programs. This means that capabilities of information weapons are not yet comparable with the power of nuclear weapons, and it is generally wrong to bet on their further build-up.

If nation-states adopt intimidation in information space as their policy, this will only lead to new upsurge in an arms race and militarization of information space.

The only reasonable alternative to this insanity is the aforementioned peace initiative in the field of international information security, furthered by the SCO member-states in the UN.

It also aims at preventing information aggression. However, in contrast to deterrence strategy it is based not on a fear of retribution, but

on a voluntary adoption by nation-states of universal rules of conduct in information space, the responsible fulfillment of which will ensure peace, stability and equal security for all peoples in the global information space.

We stand for broad international cooperation in addressing the global problem of countering the threat of unleashing of information warfare and proliferation of information weapons. With that the main aim of furthering of cooperation, in our view, is to establish an international legal regime of international information security, which would in particular regulate the military activities of nation-states in the global information space on the basis of principles and norms of international law. We stand for establishing of frameworks for bilateral and multilateral cooperation on military aspects of international information security.

Thank you for your attention!

Йозеф Шроеффл

Министерство обороны и спорта Австрии

Защита критически важной инфраструктуры в киберпространстве

Введение

Кибервойна является новой и серьезной угрозой для государств, инфраструктура которых основана на современных информационных и коммуникационных технологях (ИКТ). Поэтому необходим анализ жизненно важных инфраструктур с точки зрения потенциальных угроз, а также разработка стратегических концепций безопасности и мер противодействия возможным нападениям[1].

Уязвимость информационного общества

Работоспособность стратегически важных инфраструктур, обеспечивающих жизненно важные общественные функции, является критически важной для государства в целом. Нарушение работоспособности или разрушение этих инфраструктур может повлечь серьезные последствия для здоровья, безопасности или экономического и социального благосостояния населения, а также для эффективного функционирования государственных учреждений.

Наше «индустриальное общество» находится на пути перехода к «информационному обществу». Оно (на данный момент) зависит от промышленного производства, но в то же время стало значительно более зависимым от функционирования информационных и коммуникационных потоков. При этом оно также стало уязвимым к любым нарушениям этих потоков. Растущая зависимость информационного общества от информационных и коммуникационных систем, с одной стороны, и уязвимость этих систем с другой, создают слабые места, которые могут быть преднамеренно использованы, чтобы ослабить или даже уничтожить информационное общество или его части.

[1] Первоначально настоящая статья была написана и опубликована Вальтером Унгером под названием «Кибервойна и защита критически важной инфраструктуры» (Walter J. Unger: “Cyber War and the Protection of Strategic Infrastructure”) в книге Й. Шроеффла «Гибридная и кибервойна как следствия асимметрии» (J. Schröfl, “Hybrid and Cyber War as consequences of Asymmetrie”), Peter Lang. New York, 2011, p. 145–154. В качестве редактора этой книги Й.Шроеффл частично дополнил и доработал настоящую статью.

Массированная атака, направленная против ИКТ-систем государства или общества, при определенных обстоятельствах может иметь такие же последствия, как непосредственное нападение на промышленные предприятия.

Потенциал угрозы кибервойны[2]

Кибервойна это «намеренное выведение из строя (или искажение) информации, информационных систем и информационных процессов противника для завоевания информационного превосходства на театре военных действий, в зоне проведения операции или на поле боя — конечной целью является решение своих политико-стратегических, военно-стратегических, оперативных или тактических задач без применения традиционных военных средств или путем их дополнения».

Вероятными целями атак в кибервойне являются основы — доступность, конфиденциальность и целостность — стратегически важной инфраструктуры государства, основанной на ИКТ. Благодаря всемирной сети, атака может быть начата из любого места на Земле. Поэтому её значительно труднее отследить и идентифицировать в качестве внешней угрозы. Низкие затраты на проведение атаки расширяют круг потенциальных злоумышленников. Нападающей стороной могут быть не только государства, но также террористические группы и даже отдельные лица. Поэтому нападение на ИКТ должно расцениваться как «вооруженное нападение» в смысле статьи 51 Хартии ООН или как преступление — политическое, или общего характера. Мотивы могут быть политическими, идеологическими, религиозными, этническими, а также экономическими, анархическими, или просто личными. В общем, можно представить себе широкий спектр нападающих или преступников и их мотивов.

При проведении атак успешно используются ботнеты, вредоносное и разрушающее программное обеспечение, внедряется неисправное оборудование, а также применяются методы нарушения работы или выведения ИКТ из строя. Преимуществами для нападающего являются дешевизна средств, малая вероятность быть обнаруженным, а также независимость от времени и места. Трудно, или почти невозможно обнаружить следы подготовки нападения. Объекты нападений могут быть атакованы

---

[2] См. Walter J. Unger/Heinz Vetschera, “Cyber War und Cyber Terrorismus als neue Formen des Krieges” [Кибервойна и кибертерроризм, как новые виды войны], в: ÖMZ [Австрийский военный журнал] 2/2005, p. 204 ff.

в течение очень короткого периода времени, при этом степень физического повреждения цели может быть ограничена с целью возможной последующей эксплуатации цели.

Кроме того, общие средства и методы электронного нападения могут быть использованы одновременно с физическими атаками против критически важных ИКТ-структур (с использованием, например, зажигательных боеприпасов, бомб, оружия, использующего электромагнитные, микроволновые и лазерные технологии).

Конкретная степень потенциально наносимых повреждений может быть оценена только после детального анализа[3], поскольку, в частности, недостаточно изучена степень связанности и взаимозависимости между стратегическими ИКТ-ресурсами.

В прошлом, целями частично скоординированных нападений были сети правительств, государственных учреждений, политических партий и банков. Сценарий кибервойны кроме этого предполагает осуществление нападений на системы энергообеспечения, особенно электроснабжения, центры телекоммуникационных провайдеров, институтов внутренней и внешней безопасности, то есть полиции и армии, и против теле- и радиостанций. Скоординированные нападения, вероятно в сочетании с традиционными методами, могут парализовать страну не только на несколько часов, но и на несколько недель. Если такой подход будет реализован в рамках целостной наступательной стратегии, он может быть использован для достижения политических интересов. Поэтому все технически высокоразвитые государства должны принимать стратегические и оперативные меры, чтобы защитить себя от таких потенциальных угроз.

Уже сегодня кибервойна несет значительный неконвенциональный риск для национальной безопасности. Государственные учреждения и коммерческие предприятия, которые потенциально могут стать объектами нападения, должны быть готовы к самозащите. Преступные действия должны расследоваться в судебном или уголовном порядке. Государственные структуры безопасности могут не справиться с множеством видов преступной деятельности и её масштабами — потребуется создание специальных возможностей и сил. Во многих странах для защиты националь-

[3] Анализ должен в особенности принимать во внимание эффект домино и каскадный эффект, а также вторичный и третичный эффект/ущерб. Кроме ущерба от намеренных действий, необходимо рассматривать и возможные катастрофические разрушения стратегических ИКТ, вызванные природными силами, технической или человеческой ошибкой.

ной безопасности от внешних атак используются средства кибервойны, и, как следствие, это уже стало новой военной задачей национальной обороны.

Стратегия защиты национального киберпространства

Стратегия означает проецирование силы в политике[4], в то время как природа факторов силы имеет второстепенное значение. Заключенная в понятие «стратегической информационной войны», кибервойна практически совпадает со стратегической концепцией, разработанной Андре Бофре. В соответствии с ней, целью любой стратегии является выполнение поставленных политикой задач при наилучшем использовании имеющихся средств[5]. В бою идет поиск такого решения, которое заставит противника принять условия, налагаемые на него. В этом противостоянии воли решение становится психологической реакцией, внушаемой противнику: его необходимо убедить в бесполезности начинать или продолжать битву[6].

Если кибервойна является наступательной стратегической концепцией, потенциально угрожаемые государства (то есть все те, которые в значительной степени зависят от функционирования критически важной инфраструктуры, основанной на ИКТ) должны разработать и внедрить концепции стратегической защиты.

Ядром концепции должна быть оптимальная защита соответствующих основ ИКТ. Первостепенное значение имеет постоянная доступность, надлежащая конфиденциальность, и не нарушаемая целостность (базовые ценности ИКТ) подлежащих защите информационных услуг и линий связи критически важных ИКТ — в особенности, высокая доступность критически важной ИКТ-инфраструктуры (близкая к 100%).

Варианты стратегии

В принципе, доступны следующие стратегические варианты защиты от нападения[7] в ходе кибервойны:

---

[4] См. W.J. Unger/Heinz Vetschera, „Cyber War und Cyber Terrorismus als neue Formen des Krieges“, ÖMZ 2/2005, S. 203 ff.

[5] См. André Beaufre, Totale Kriegskunst im Frieden — Einführung in die Strategie [Искусство тотальной войны в мирное время — введение в стратегию]; Berlin, 1963; p. 25.

[6] Ibid.

[7] См.: Lukasik, Goodman, Longhurst “Protecting Critical Infrastructures Against Cyber-Attack”, ADELPHI PAPER 359, Oxford 2003, p. 5ff.

1) Защита посредством сдерживания и превентивных мер;

2) Постоянная защита критической инфраструктуры и принятие мер предосторожности на случай чрезвычайных ситуаций и кризисов для недопущения достижения злоумышленником политических целей;

3) Принятие быстрых мер по ограничению масштабов ущерба;

4) Возможность быстрого восстановления поврежденных систем посредством антикризисного управления.

В настоящее время защита посредством сдерживания и превентивных мер не является вариантом для небольших государств, так как для этого нет соответствующих предпосылок, в то время как варианты №3 и №4 допускают причинение большого ущерба и, следовательно, неприемлемы для уверенного в своих силах государства, идущего по пути в информационную эпоху. В этом случае нужно следовать варианту №2, а именно обеспечивать постоянную защиту критической инфраструктуры и принимать меры предосторожности на случай чрезвычайных ситуаций и кризисов для недопущения достижения злоумышленником политических целей. Шансы на успех этого варианта главным образом зависят от владельцев и операторов критически важных инфраструктур, так как основная их часть находятся в частных руках.

Государство также несет ответственность по защите общества в киберпространстве. Нужно стремиться к реализации варианта №2, создавая предпосылки, рамочные условия, а также выделяя необходимые ресурсы. В этом контексте объектами защиты являются критически важные инфраструктуры государства, зависящие от ИКТ.

Виды кибератак в войне

Если в будущем начнется война между крупными мировыми державами, первой жертвой конфликта может стать сам Интернет. Конечная цель военных действий — достижение победы — останется неизменной, и военные стратегии Сунь-Цзы и Клаузевица по-прежнему будут применимы. Тем не менее, многие виды военной тактики претерпят изменения с учетом уникальной природы киберпространства и скрытой силы кибероружия. В войне будет две обширных категории кибератак.

Вооруженные силы

Кибератаки первой категории будут проводиться как часть общих действий по выведению из строя оружия противника и нарушению работы военных систем командования и управления.

Разумно предположить, что в случае крупной региональной или мировой войны такого рода атаки померкнут в сравнении с уровнем сложности и масштабами тех киберинструментов и тактик, которые государства, скорее всего, имеют в резерве на случай кризиса национальной безопасности.

Критически важная инфраструктура

Кибератаки второй категории будут направлены на способность и готовность противника вести войну в течение длительного периода времени. Цели, скорее всего, будут включать в себя финансовый сектор, промышленность и национальное самосознание противника[8]. Критически важными являются инфраструктуры[9] или их части, которые имеют существенное значение в обеспечении важных социальных функций. Их нарушение или разрушение оказывает серьезное влияние на здоровье, безопасность или экономическое и социальное благосостояние населения, или на эффективное функционирование государственных учреждений.

На основе Европейской программы по защите критически важной инфраструктуры[10] в Австрии на национальном уровне был разработан генеральный план — Австрийская программа защиты критически важной инфраструктуры (APCIP). В ней рассмотрены принципы программы, приведены списки приоритетных секторов для проведения расследований, определены критерии оценки критически важных инфраструктур, выделены факторы риска и акторы, приведен список мер по защите критически важных инфраструктур и выработан план действий с подробным описанием задач.

В Европейской программе перечислены 11 отраслей критически важной инфраструктуры[11]: энергетика, атомная промышленность, ИКТ, водоснабжение, снабжение продовольствием, здравоохранение, финансы, транспорт, химическая промышленность, космонавтика, научно-исследовательские институты.

---

[8] См. Также Кеннет Гирс «Демистификация кибервойны» (Kenneth Geers: “Demystifying Cyber Warfare”) в книге Й.Шроеффла «Гибридная и кибервойна как следствия асимметрии» (J. Schröfl, “Hybrid and Cyber War as consequences of Asymmetrie”), Peter Lang. New York, 2011, p 119 — 126.

[9] Common Report of the Federal Chancellor and the Ministry of the Interior Concerning the Austrian Program for Critical Infrastructure Protection; Master Plan APCIP; Ministerial Council Resolution of 02 April 2008, p. 1.

[10] EPCIP = European Program for Critical Infrastructure Protection.

[11] См. там же, Common Report of the Federal Chancellor..., p. 5.

Не все из этих секторов имеют для Австрии такую же значимость, как для ЕС. Атомная промышленность и космонавтика не имеют конкретной национальной значимости. При этом, в австрийской критически важной инфраструктуре сделан акцент на государственные учреждения, обслуживание социальной системы и системы обороны, а также на службы оперативного реагирования.

Центры, узлы связи и системы управления этих критических инфраструктур, находящихся в распоряжении современного общества, функционируют на основе информационных и коммуникационных технологий или имеют большое значение для ИКТ и могут эксплуатироваться только в определенных местах.

Последствия

Государство должно вносить вклад в поддержание возможности по защите стратегически важной ИКТ-инфраструктуры от кибератак — путем предоставления постоянно доступных и актуальных прогнозов ситуации, сделанных на основе периодического анализа и оценки рисков безопасности; создания системы раннего предупреждения, дополненной функционалом реагирования в чрезвычайных ситуациях, а также соответствующими полномочиями.

Незаменимым является интенсивное сотрудничество на национальном уровне между промышленностью, учеными, правительством и гражданами (государственно-частное партнерство). Оно должно быть инициировано и продвигаться государством. На европейском уровне государства должны, в частности, сотрудничать по вопросам профилактики, выявления угроз и обороны.

Владельцы и операторы критически важной инфраструктуры должны создать предпосылки для безопасной деятельности — реализовать комплексные меры по защите от внешних и внутренних атак, наладить обмен информацией, сотрудничество между операторами, поддерживать высокие стандарты безопасности и проводить авторизованные курсы для персонала. Многообещающими подходами являются разработка и использование систем, «устойчивых к вторжениям», резервирование, автоматизация критических процессов с перекрывающим ручным управлением.

В областях с особыми требованиями к безопасности следует использовать исключительно проверенное или соответствующим образом сертифицированное программное и аппаратное обеспечение, организации, процедуры и надежный персонал. Защита

важных данных и структур должна осуществляться в соответствии с законом, сообразно уровню важности ИКТ и масштабами угроз.

Критически важным инфраструктурам необходима постоянная базовая защита с активными и пассивными мерами, соответствующий персонал и материалы. Защита должна быть организована таким образом, чтобы в случае предполагаемой опасности от катастроф, террористических актов, военных действий её можно было быстро усилить.

Планы на случай чрезвычайных ситуаций должны постоянно актуализироваться в ходе периодических учений и все участники должны быть обязаны поддерживать высокую осведомленность о требованиях мер безопасности, рисках и необходимых контрмерах.

В принципе, меры безопасности должны быть организованы в соответствии с девизом «защитить, выявить, отреагировать» и разделяться на оборонительные и наступательные меры. Понятно, что в критических и неоднозначных ситуациях ИКТ-системы играют особую роль с точки зрения их собственной информации и поддержки.

Необходимость правовых адаптаций

На национальном уровне должны быть четко определены и наделены соответствующими полномочиями компетентные органы в области превентивной обороны и противодействия атакам из киберпространства, направленным против «критически важных ИКТ-структур». Для предотвращения злоупотреблений и улучшения отношения к этим необходимым мерам необходимо обеспечить эффективную правовую защиту и механизм контроля.

С точки зрения международного права атака посредством информационных технологий, вероятно, может квалифицироваться как «вооруженное нападение» в понимании Устава ООН[12]. Квалификация «вооруженного нападения» зависит в первую очередь не от используемых средств, а от намерения нанести вред и степени фактического ущерба. Так как существенный ущерб, сравнимый с ущербом от вооруженного нападения, может быть нанесен, в частности, с помощью информационных технологий, нападения из киберпространства, безусловно, могут считаться «вооруженным нападением» в смысле статьи 51 Устава Организация

---

[12] См. W.J. Unger/Heinz Vetschera, “Cyber War und Cyber Terrorismus als neue Formen des Krieges” [Кибервойна и кибертерроризм как новые формы войны], in: ÖMZ [Австрийский военный журнал] 2/2005, p. 209 ff.

Объединенных Наций, которая легитимирует право потерпевшей стороны на самооборону. Также необходимо уточнение, какие обязательства будут иметь нейтральные государства в случае, если через их «национальное киберпространство» осуществлены атаки в отношении третьих сторон.

Выводы

Государство должно обеспечить достаточные ресурсы для создания инструмента, который позволил бы осуществлять анализ, оценку и прогнозирование изменений в стратегических ИКТ, в том числе оценку рисков, а также для создания постоянного ситуационного центра для наблюдения, оценки уровня угрозы и, при необходимости, для раннего предупреждения, приведения в готовность, реагирования и задействования экстренных служб (CERT/CSIRT = группа реагирования на компьютерные происшествия / группа реагирования на инциденты, связанные с компьютерной безопасностью).

Развитому государству необходим центральный орган, который собирает, анализирует и оценивает всю необходимую информацию, поступающую от федеральных и местных учреждений, а также от частных лиц, и который в состоянии сам принимать необходимые меры по наблюдению, профилактике, обороне и реагированию, или, соответственно, может потребовать их принятия. Целесообразно, чтобы этот орган также обеспечил управление и координацию сотрудничества на национальном и международном уровне. Для этого должны быть созданы необходимые правовые предпосылки.

Joseph Schroeffl
Ministry of Defence and Sports, Austria

Protection of Critical Infrastructure in Cyber Space

Introduction

Cyber War (CW) is a new and serious form of threat for states whose infrastructure is based on modern information and communication technologies (ICT). It is therefore indispensible to analyze vital infrastructures with regard to potential threats to them and to develop strategic security concepts as well as measures against possible attacks[1].

Vulnerable Information Society

The functioning of strategically relevant infrastructures to maintain vital societal functions is critical for the state as a whole. Disruptions or destructions of these infrastructures have serious consequences for the health, security, or economic and social wellbeing of the population as well as for the effective functioning of national installations.

Our "industrial society" is on the way of becoming an "information society". It (still) depends on industrial production but has, meanwhile, become considerably *dependent* on functioning information and communication flows. But with that it has also become *vulnerable* to any disruptions of these flows. Information society's increasing dependence on information and communication systems on the one hand and the vulnerability of these systems on the other, create week points which can be intentionally used to weaken or even destroy an information society or parts thereof.

A massive attack against the ICT systems of a state or a society may, under certain circumstances, have the same consequences as an attack against the industrial basis itself.

---

[1] This article has originally been written and published by Walter J. Unger: "Cyber War and the Protection of Strategic Infrastructure" in J. Schröfl, aO: "Hybrid and Cyber War as consequences of Asymmetrie", Peter Lang. New York, 2011, p. 145–154. As Editor of the book I partly amended, rounded up and completed this article into the present shape. Thank You Walter!

The Threat Potential of Cyber War[2]

Cyber War (CW) is "the intentional impairment of enemy information, information systems and information-supported processes, in order to gain information superiority in the theater, area of operation or on the battlefield, with the ultimate goal of enforcing own politico-strategic, military-strategic, operational or tactical goals, by avoiding or supplementing the use of traditional military means".

Likely targets of CW attacks are the basic values — availability, confidentiality, and integrity — of the strategic ICT-based infrastructures of a state. Due to the worldwide web, an attack can be launched from any place on earth. This makes it considerably harder to trace and identify it as an external threat. The low costs of carrying out an attack extend the scope of potential perpetrators. Not only states but also terrorist groups and even individual persons can be attackers. Therefore attacks against ICT will have to be rated as "armed attack" in the sense of Article 51 of the UN Charta or as a political or general "criminal act". The motives can be political, ideological, religious, ethnic as well as economic, anarchic or merely personal. All in all, one can imagine a broad spectrum of attackers or perpetrators and their motives.

What is useful in carrying out attacks are botnets, malicious and damage-inflicting software, the introduction of faulty hardware as well as methods to disrupt or paralyze the ICT. Advantages for the attacker are the inexpensive means, the small probability of being discovered as well as being independent of time and place. The preparation of an attack is difficult if not impossible to notice. The targets of the attacks can be hit within a very short period of time and with a view to possibly intended subsequent use the extent of the physical damage of targets can be limited.

In addition, the common means and methods of an electronic attack can be employed simultaneously with physical attacks against critical ICT structures (e.g. incendiary attacks, bombs, EMP, microwave and laser technology).

The concrete extent of potentially causable damage can only be assessed after a detailed analysis[3], since especially the extent of the

---

[2] see Walter J. Unger/Heinz Vetschera, "Cyber War und Cyber Terrorismus als neue Formen des Krieges" [Cyber War and Cyber Terrorism as New Forms of War], in: ÖMZ [Austrian Military Journal] 2/2005, p. 204 ff.

[3] An analysis has to especially take into account domino effects and cascade effects as well as secondary and tertiary effects/damages. Aside from threats caused by deliberate acts, also the catastrophic damages of the strategic ICT caused by a higher power, technical or human error have to be taken into consideration.

networking and the respective dependencies between the strategic ICT resources are not sufficiently known.

Targets of partly coordinated attacks in the Past were the nets of the government, governmental offices, political parties, and banks. A cyber war scenario would emerge if additional attacks were launched against energy supply installations, especially electricity supply, the centers of telecommunication providers, the security instruments for internal and external security, i.e. the police and the military and against television and radio stations. Coordinated attacks, probably combined with traditional methods, could paralyze a country not only for hours but for weeks. If embedded in a holistic offensive strategy, political interests could be enforced. All technically highly advanced states therefore have to take strategic and operational precautions to protect themselves against such potential threats.

Already today, CW presents a substantial sub-conventional risk for national security. Potentially affected government agencies and business enterprises have to provide for self-protection. Criminal acts are to be legally prosecuted. Type and extent of criminal acts could overchallenge governmental security installations and require special capabilities and forces. In many countries defense against attacks on national security from outside, using CW means, has consequently become a new task of military national defense.

Strategy for the Protection of National Cyber Space

Strategy means translating power into politics[4], while the nature of the power factors is of secondary importance. Embedded in a "strategic information war", CW is almost identical with the strategic concept developed by Beaufre. According to that, it is the aim of every strategy to fulfill the tasks set by politics with the best possible use of the available means[5]. The decision sought in battle is to make the opponent accept the conditions imposed on him. In this dialectic of wills the decision becomes a psychological reaction to be instilled in the opponent: He should become convinced that it is useless to take up battle or continue it[6].

[4] Cf. W.J. Unger/Heinz Vetschera, „Cyber War und Cyber Terrorismus als neue Formen des Krieges", ÖMZ 2/2005, S. 203 ff.

[5] Cf. André Beaufre, Totale Kriegskunst im Frieden — Einführung in die Strategie [Total Art of War in Peacetime — Introduction into Strategy]; Berlin, 1963; p. 25.

[6] Ibid.

If CW is the offensive strategic concept, potentially threatened states — i.e. all those which, to a substantial degree, depend on a functioning critical information and communication technology-based infrastructure — have to develop and implement strategic protection concepts.

The core of the concepts must be the optimal protection of the relevant ICT basic values. What is of primary importance is all-time availability, appropriate confidentiality, and inviolable integrity (ICT basic values) of the wanted information services and communication lines of critical ICT — in particular the high-availability of critical ICT infrastructure (close to 100%).

Strategic Options

In principle, the following strategic options for the protection against a CW attack[7] are available:

1) Prevention through deterrence and precaution;

2) Preventing the attacker from reaching his political goals by permanently guarding the critical infrastructure and taking precautions for emergencies and crises;

3) Confining damage by taking fast measures to limit the extent of damage;

4) Capability to quickly restore damaged systems through crisis management.

Prevention through deterrence and precaution is, at present, not an option for small states, as the preconditions for that are not there, while options 3 and 4 allow for the infliction of great damage and should therefore not be acceptable for a self-confident state on its way into the information age. Option 2, namely to prevent the attacker from reaching his goals by permanently protecting the critical infrastructure and taking precautions for emergencies and crises should, in any case, be sought. The chances for success of this option depend mainly on the owners and operators of critical infrastructures, since the bulk of these are in private hands.

The state also has the responsibility toward society to protect it in cyber space. By creating the prerequisites, framework conditions, and providing the necessary resources, option 2 has to be pursued resolutely. In this context the objects of protection are the country's critical ICT-dependent infrastructures.

---

[7] 15 Cf.: Lukasik, Goodman, Longhurst "Protecting Critical Infrastructures Against Cyber-Attack", ADELPHI PAPER 359, Oxford 2003, p. 5ff.

Cyber-Attack Categories in War

If there is a future war between major world powers, the first victim of the conflict may be the Internet itself. The ultimate goal of warfare — victory — will not change, and the military strategies of Sun Tzu and Clausewitz will still apply. However, many war tactics will change in order to account for the unique nature of cyberspace and the latent power of cyber warfare. There will be two broad categories of cyber-attacks during the war.

Military forces

The first category of cyber-attacks would be conducted as part of a broader effort to disable the adversary's weaponry and to disrupt military C2 systems.

In the event of a major regional or world war, it is wise to assume that these kind of attacks would pale in comparison to the sophistication and scale of cyber tools and tactics that governments likely hold in reserve for a time of national security crisis.

Critical infrastructure

The second category of cyber-attacks would target the adversary's ability and willingness to wage war for an extended period of time. The targets would likely include an adversary's financial sector, industry, and national morale[8]. Critical Infrastructures[9] are those infrastructures, or parts thereof, which are of substantial relevance in maintaining important societal functions. Their disruption or destruction has serious effects on the health, security or the economic and social wellbeing of the population or on the effective functioning of governmental installations.

On the basis of the European Program for Critical Infrastructure Protection[10] a master plan was elaborated also for Austria on the national level — the Austrian Program for Critical Infrastructure Protection (APCIP). It describes the principles of the program, includes listings of those sectors that have priority to be investigated, defines the criteria for rating critical infrastructures, identifies the risk factors and

---

[8] See also Kenneth Geers: "Demystifying Cyber Warfare" in J. Schröfl, aO: "Hybrid and Cyber War as consequences of Asymmetrie", Peter Lang. New York, 2011, p 119 — 126.

[9] Common Report of the Federal Chancellor and the Ministry of the Interior Concerning the Austrian Program for Critical Infrastructure Protection; Master Plan APCIP; Ministerial Council Resolution of 02 April 2008, p. 1.

[10] EPCIP = European Program for Critical Infrastructure Protection.

the actors, lists the measures for the protection of critical infrastructures, and develops an action plan with detailed sub-goals.

The European program lists 11 sectors of critical infrastructures[11]: energy, nuclear industry, ICT, water, victuals, health, finances, transport, chemical industry, space travel and research institutions.

For Austria not all of these sectors have the same relevance as for the EU. Nuclear industry and space travel are of no specific national relevance. Conversely, in Austria's national critical infrastructure emphasis is also put on constitutional installations, the maintenance of the social system and the defense systems as well as on first responder organizations.

The centers, communication nodes and steering systems of these critical infrastructures at the disposal of a modern society are based on information and communication technology or are of considerable importance for the ICT and can only be operated in certain locations.

Consequences

The state should help maintain the capability to protect strategic ICT infrastructure against cyber attacks by means of permanently available and up-to-date estimates of the situation on the basis of periodic analyses and assessments of the security risks, an early warning system, complemented by emergency/incident functionalities, as well as by the ability to react appropriately.

Intensive cooperation on national level between industry, science, administration, and citizens (Private — Public — Partnership) is indispensible and has to be initiated and promoted by the state. On the European level states would have to cooperate particularly in prevention, threat identification, and defense.

The owners and operators of critical infrastructures have to create the preconditions for the secure operation by comprehensive protection measures against attacks from outside and from inside, exchanging information, cooperation between the operators, maintaining high security standards and certified training of their personnel. To develop and use "intrusion-tolerant" systems, redundant design, automated critical processes with super-imposed manual steering are approaches that promise success.

For security-critical areas one should exclusively use accredited, or respectively, certified hard and software, organizations, procedures, and reliable personnel. Protection-worthy data and locations accord-

[11] Cf.. loc cit, Common Report of the Federal Chancellor..., p. 5.

ing to the criticality of the ICT and the extent of the threat are to be protected in conformity with the law.

Critical infrastructures require permanent basic protection with active and passive measures, personnel, and material. The protection has to be set up in a way that in the event of assumed danger through catastrophes, terrorist attacks, or war operations it can be quickly reinforced.

Emergency plans have to be kept up-to-date through periodic exercises and everybody involved has to be forced to maintain high security awareness about the risks and necessary countermeasures.

As a principle, the security measures are to be established according to the motto "protect, identify, react" and be divided into defensive and offensive measures. It is clear that ICT systems play a special role with regard to own information and support in critical and obscure situations.

Need for Legal Adaptations

On the national level, the competent authorities in the area of preventive defense and the fight against attacks from cyber space launched against "critical ICT structures" have to be clearly established, and those organs are to be vested with appropriate authority. To prevent misuse and raise the acceptance of these necessary measures, effective legal protection and a control mechanism would have to be established.

Relating to international law, an attack with means of information technology may probably qualify as "armed attack" in the sense of the UN statutes[12]. The qualification of "armed attack" is not primarily a matter of the means used as such but rather of the intention to inflict harm and the extent of the actual damage. Since particularly also with means of information technology substantial damage can be done, which does not fall short of that incurred by an armed attack, attacks from cyber space could certainly be considered "armed attacks" in the sense of article 51 of the statutes of the United Nations, which legitimizes the attacked to exercise his right of self-defense. In addition, it would have to be clarified what obligations a neutral state would have if, via its "national cyber space", attacks are launched against third parties.

---

[12] Cf. W.J. Unger/Heinz Vetschera, "Cyber War und Cyber Terrorismus als neue Formen des Krieges" [Cyber War and Cyber Terrorism as New Forms of War], in: ÖMZ [Austrian Military Journal] 2/2005, p. 209 ff.

Conclusions

The state has to provide adequate resources for an instrument to analyze, assess, and predict developments in strategic ICT, including risk assessment, a permanent situation center for observation, estimate of the threat situation and, if necessary, for early warning, alert, and activation of reactions and emergency organizations (CERT/CSIRT= Computer Emergency Response Team/ Computer Security Incident Response Team).

What a developed state needs is a central authority which collects, analyzes, and assesses all pertinent information from federal and provincial offices as well as from private parties and which is in the position to take the necessary reconnaissance, prevention, defense, and reaction measures, or respectively, can order them obligatorily. This authority would expediently also ensure steering and coordination of national and international cooperation. The necessary legal preconditions for that would have to be established.

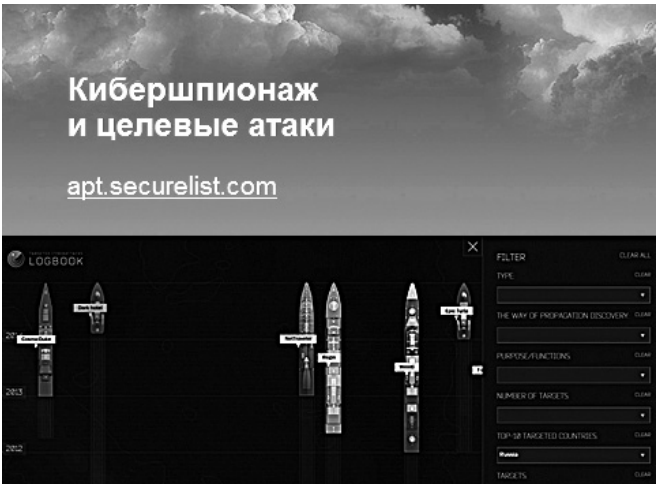
А.Ю.Ярных
Лаборатория Касперского

Уязвимости каждого дня, развитие информационных угроз

Я хотел бы начать доклад с небольшой ретроспективы компьютерных угроз, которые мы наблюдали в динамике все эти годы. Начиная с 1994 года, цифрой дня была «1 новый вирус каждый час», в 2006 году уже «1 новый вирус каждую минуту», в 2011 стало уже «1 новый вирус каждую секунду». Не имея возможности уменьшать временной интервал далее, мы в 2014 году можем просто констатировать, что каждый день добавляет 325 000 образцов вредоносного ПО.

Далее продолжу сравнение эпох развития киберугроз, от элементарных и сравнительно безобидных образцов вредоносного кода 1990 годов, написанного для самоутверждения или в хулиганских целях, до 2010 года, когда программы стали совершенными, целевыми и написаны преимущественно с целью кражи денег или информации. И опять мы видим эволюционные признаки от простого к сложному, видим как рост числа пользователей сети Интернет и проникновение технологий в нашу жизнь используется злоумышленниками для наращивания вредоносного потенциала.

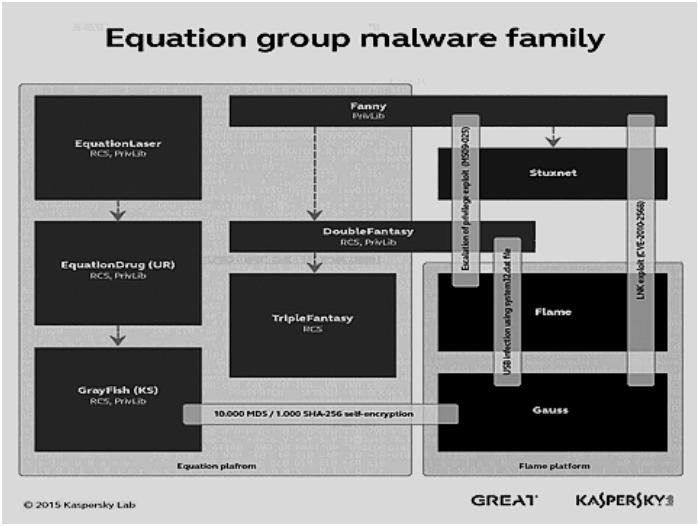
Некоторой вершиной этого развития становятся наиболее сложные и совершенные программы, часть из которых уже вполне можно классифицировать как «кибероружие». Это программы, сочетающие мощный и развитый шпионский функционал и имеющие потенциал к деструктивной деятельности, вплоть до разрушений критически важной инфраструктуры. Собрав данные о таких программах, мы открыли специальный ресурс на страничке https://apt.securelist.com/, на котором мы графически отображаем историю, территориальную активность, количество заражений и взаимосвязи программ категории APTs (advanced persistent threats).



Взаимосвязи этих программ хорошо видны также на следующем слайде, на котором показаны взаимосвязи Equation Group. Инфраструктура Equation Group включает в себя более 300 доменов и 100 контрольно-командных серверов, расположенных в разных странах, в частности в США, Великобритании, Италии, Германии, Нидерландах, Панаме, Коста-Рике, Малайзии, Колумбии и Чехии.

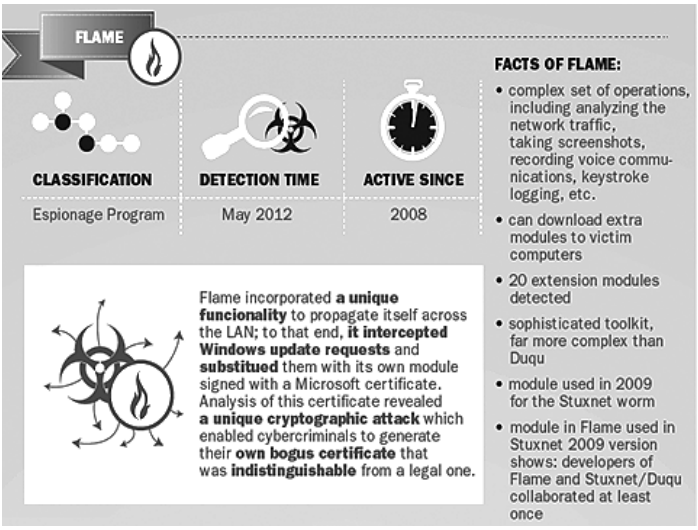
Лаборатория Касперского установила, что Equation Group взаимодействовала с другими кибергруппировками, в частности с организаторами нашумевших кампаний Stuxnet и Flame. По всей вероятности, Equation Group делилась с «коллегами» имевшимися у нее эксплойтами, использующими уязвимости нулевого дня. Например, в 2008 году червь Fanny применял те эксплойты, которые появились в Stuxnet только в июне 2009-го и марте 2010-го, при этом одним из этих эксплойтов являлся модулем Flame.

Как выяснили наши эксперты, на начальной стадии заражения Equation Group может использовать до 10 эксплойтов, однако на практике редко применяется больше трех. Пробуя по очереди три разных эксплойта, группировка пытается проникнуть в систему, но, если все три попытки не увенчиваются успехом, атакующие отступают.

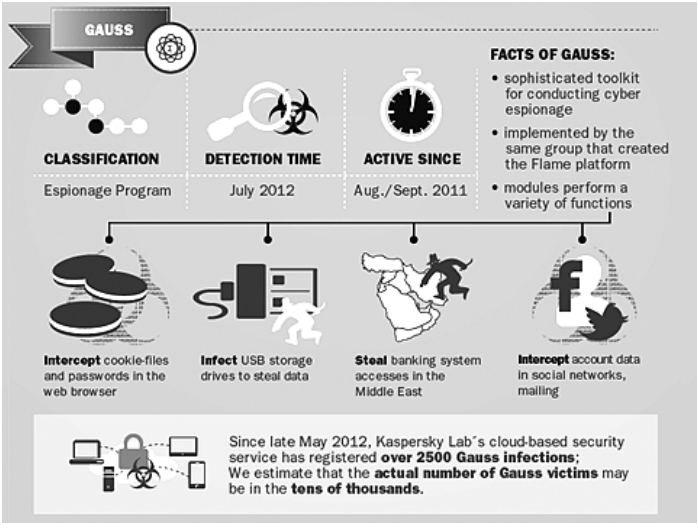


Далее на слайдах представлен функционал двух наиболее интересных вредоносных программ, с которыми нам приходилось сталкиваться в работе. Это Flame, который является фактически

развитым конструктором для кибершпионажа, в нем найдены модули, которые ранее использовались в Stuxnet.

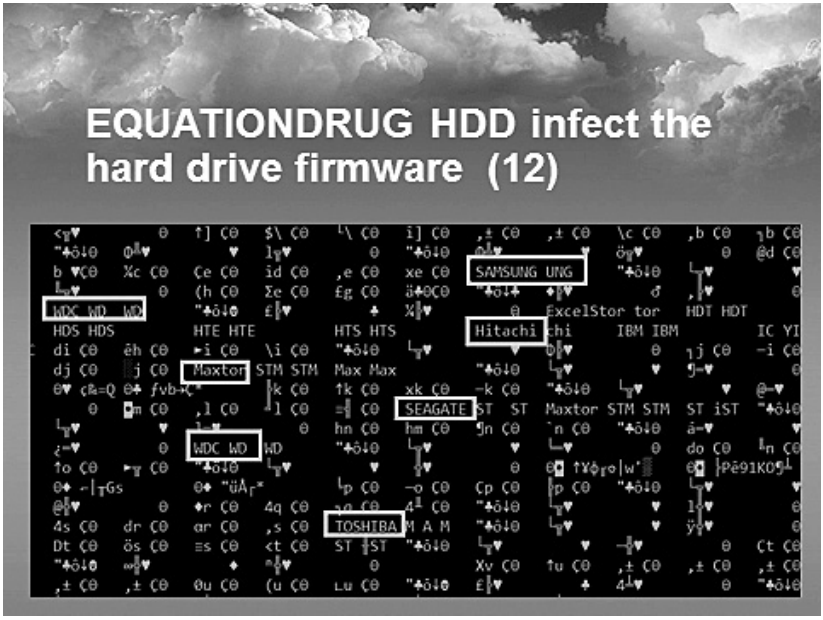


И далее вредоносная программа Gauss, которая дополнительно имеет богатый функционал по распространению в социальных сетях. Также были выявлены интересные возможности по заражению, хранению и передаче данных через USB-флэшкарты.



Возвращаясь к более новым вредоносным программам, интересен вот этот слайд, на котором выделены названия компаний, которые являются производителями жестких дисков.

В арсенале Equation Group имеется множество зловредов, и некоторые из них крайне новаторские. К примеру, Лаборатория Касперского впервые в своей практике обнаружила модули, которые позволяют перепрограммировать операционную систему жестких дисков 12 основных производителей. Надо понимать, что таким образом злоумышленники добиваются двух целей: во-первых, однажды попав в ОС жесткого диска, зловред остается там навсегда — его невозможно ни обнаружить, ни избавиться от него: он не может быть удален даже в случае форматирования диска. Во-вторых, у атакующих есть возможность создать себе «тихую гавань» в виде секретного хранилища, где может безопасно собираться вся необходимая информация.



Далее я хотел бы показать карту распространения Equation Group и категории инфраструктуры которые подвергались заражениям. Видно, что наиболее активно были атакованы Иран, Россия, Афганистан и Пакистан. В зоне особого риска оказались компьютеры военных, финансовых, государственных, дипломатических, энергетических, образовательных, телекоммуникационных и аэрокосмических структур.

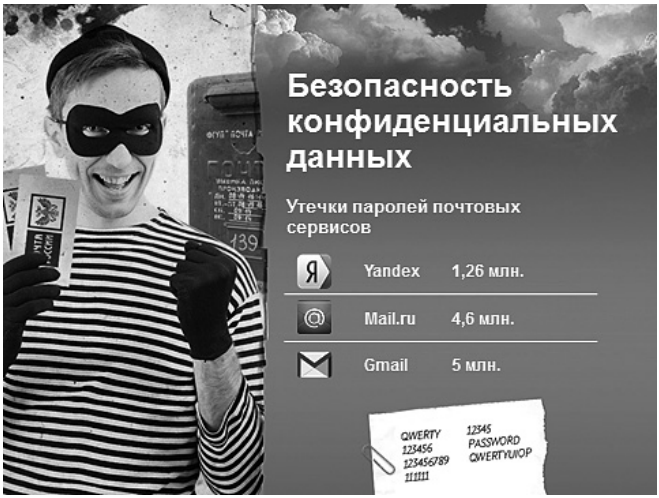
Несколько цифр в продолжение слайдов о кибершпионаже. По нашим данным, с 2013 по 2014 г. число целевых атак (APTs) увеличилось в 2,4 раза и достигло 4400 инцидентов.

Число атак на бизнес с использованием офисных приложений возросло на 75%.

Потери бизнеса в России от кибератак в среднем составляют 20 млн руб. в компаниях крупного бизнеса и порядка 780 тыс. руб. в средних и малых компаниях. 1/3 компаний при таких атаках теряла конфиденциальные данные. При этом необходимо учитывать что большинство компаний не стремятся раскрывать информацию о том, что они стали жертвами кибермошенников и понесли ущерб от их деятельности. 91% компаний признали, что прекратили бы работать с финансовой организацией, которая стала жертвой кибератаки.

Еще несколько цифр. Пользователи России, финансовые угрозы: 2013 год — 6 млн атак, 2014 год — 8 млн атак. Мобильные угрозы: более 1300 тыс. уникальных атак, из которых 53% с использованием мобильных банковских троянских программ. Каждый пятый пользователь Android столкнулся за прошлый год с киберугрозой. Из позитива можно отметить только то, что на 12% стало меньше мобильного спама.

В прошлом году в связи с утечками персональных данных и благодаря большому количеству данных с зараженных компьютеров в руках злоумышленников оказалось 1,26 млн аккаунтов почтовый службы Яндекс, 4,8 млн Mail.ru и более 5 млн Gmail.

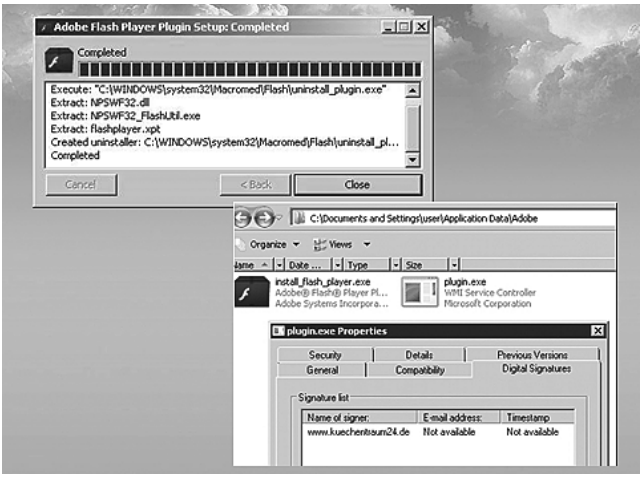


При анализе утечки был составлен список наиболее часто используемых паролей, среди которых лидируют 12345, qwerty, password и даты рождения пользователей или номер телефона, т.е. данные, которые легко получить в социальной сети.

Еще один вид угроз связан с публичными Wi-Fi-сетями.

Вот, например, в нашем отеле пароль доступа состоит из названия отеля и года, судя по всему, когда последний раз его меняли. По нашим данным, подключившись к публичной сети Wi-Fi, 26% пользователей авторизуются в социальных сетях, а еще 41% опрошенных хранит на своих устройствах логины и пароли от почтовых и социальных аккаунтов. Приведу сценарий заражения вредоносной программой Darkhotel. После заселения в гостиницу — при подключении к публичной Wi-Fi сети, которая была предварительно взломана или специально развернута злоумышленниками — запрашивается номер пользователя и его ФИО.

Далее пользователю предлагают установить «необходимое» обновление программы, которое включает в себя исполняемый модуль вредоносной программы, обычно инсталлятор бэкдора. В данном примере, был использован обычный рабочий модуль обновления программы Adobe Flash Player, к которому был добавлен в пакет установки модуль plugin.exe, который содержал троянскую программу.



После этого злоумышленники получали доступ ко всей информации, которая была на компьютере, включая доступ к учетным записям социальных сетей, логины и пароли почтовых служб или доступ к банковским аккаунтам.

Масштаб действий киберпреступников никак нельзя недооценивать, на следующем слайде я хотел бы показать, что были примеры, когда целые страны становились жертвой кибератак. В данном примере угроза пришла через образовательную сеть и в короткий промежуток времени были заражены компьютеры государственных и финансовых служб.

В заключение я хотел бы привести некоторые советы, которые, конечно, элементарны и скорее ориентированы на обычных пользователей, а не на специалистов в области информационной безопасности:

Полезные советы от Лаборатории Касперского:

- Создайте специальную карту для онлайн-покупок и не держите на ней большую сумму денег.
- Не переходите на сайты по ссылкам в почтовых сообщениях, сообщениях в социальных сетях и чатах или кликнув по рекламному баннеру на сомнительном сайте.
- Финансовые организации никогда не присылают писем с просьбой отправить им свои личные данные в электронном сообщении, перейти на сайт для авторизации или ввести личные данные во всплывающих окнах. Не переходите на сайт по ссылкам, присланным от имени банковских организаций и платежных систем.
- Не переходите ни по каким ссылкам, присланным незнакомыми людьми.
- Избегайте магазинов, зарегистрированных на бесплатных хостингах.
- Если сайт магазина вызывает сомнения, исследуйте на сервисах whois данные о времени существования домена, на котором размещен сайт, его владельце. Обратите внимание, на какой срок оплачен домен.
- Вводите адрес банка или платежной системы вручную.

- Внимательно проанализируйте URL-страницы с полями ввода конфиденциальных данных. Если интернет-адрес состоит из бессмысленного набора символов или URL выглядит подозрительно, не оформляйте на странице с этим адресом платеж.
- Проверяйте, используется ли при передаче ваших конфиденциальных данных шифрованное соединение. Если соединение защищенное, адрес сайта должен начинаться с https, а в адресной строке или строке состояния браузера должна быть иконка закрытого замочка.
- Старайтесь не пользоваться услугами онлайн-банкинга или делать онлайн-покупки в публичных местах (интернет-кафе, клубах, библиотеках). На таких компьютерах могут быть установлены различные шпионские программы, считыватели нажатий клавиш, перехватчики интернет-трафика. Даже если вы пользуетесь своим компьютером, но при этом осуществляете банковские операции по публичной бесплатной сети Wi-Fi, существует риск перехвата трафика администратором этой сети, прослушивания посторонними лицами и атак с использованием сетевых червей — особенно, если сеть Wi-Fi не защищена паролем.
- Всегда держите вашу операционную систему и антивирусное ПО в актуальном состоянии. Используйте на компьютере антивирусную программу с защитой от фишинга.

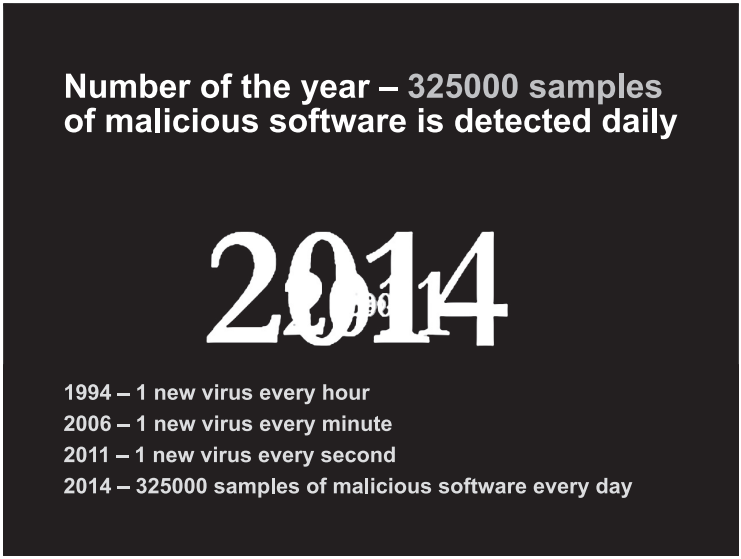
Будучи внимательным и соблюдая все меры предосторожности, можно с комфортом пользоваться всеми удобствами, которые предоставляет Интернет.

И пару слов о будущем: Основные угрозы, которые получат свое дальнейшее развитие в ближайшем будущем: прогноз экспертов Лаборатории Касперского.

A.J.Yarnyh
Kaspersky Lab Russia

Every day vulnerabilities, major trends for 2015

I would like to start the presentation with a small retrospective of computer threats, which we have observed in dynamics through all these years. Since 1994, the figure of the day was «1 new virus every hour», in 2006 it was already «1 new virus every minute», in 2011 — «1 new virus every second». Not being able to reduce the time interval any further, in 2014, we can simply say that every passing day brings about 325,000 samples of malware.



Going forward, I will continue the comparison of periods of cyber threats evolution, from elementary and relatively harmless samples of malicious code of 1990, written for self-assertion or hooliganism purposes, up to 2010, when software became perfect, targeted and created primarily for theft of money or information. And again we see the signs of evolution from simple to complex, we see as an increase in number of Internet users and penetration of technology in our lives is used by attackers for development of malicious capacity.

COMPARISON OF EPOCHS

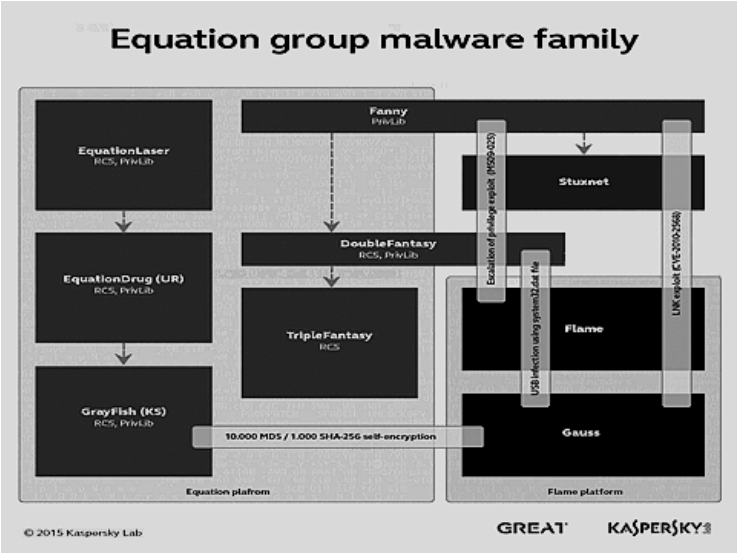
1990-е	2000-е	2010-е
Self-replicating viruses and worms	Botnet Era	Targeted attacks
Hooliganism	From hooliganism to profits	Money and data theft
Hackers studied different OS-es	Windows – target #1	Everything is a target – from a smartphone to a refrigerator
Disks, BBS	Mail, Flash-drives, vulnerabilities	Browser attacks
	Internet users	
16 mn.	***36 mn.***	***3 bln.***

The pinnacle of this development is the most complex and sophisticated software, some types of which it is already quite possible to classify as «cyberweapons». This software combines powerful and advanced spying functionality and also has a destructive potential — going up to destruction of critical infrastructure. Having gathered data on these programs, we opened a special resource page at https://apt.securelist.com/, where we graphically display history, territorial activity, the number of infections and interconnections between APTs (advanced persistent threats).

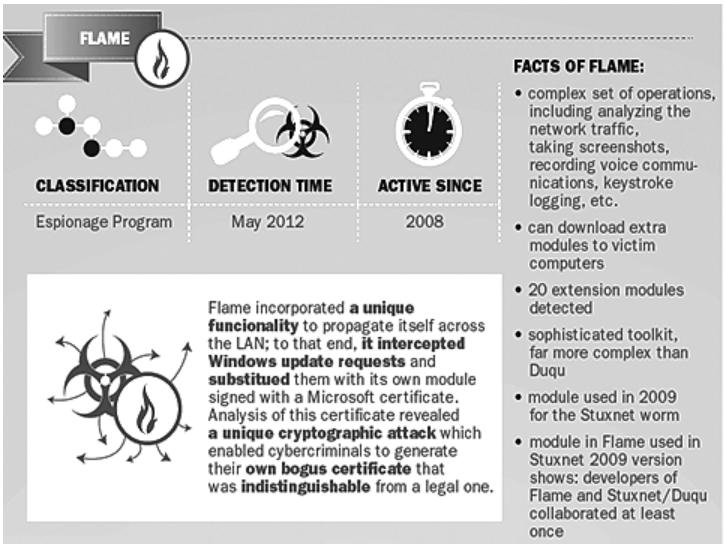
The interconnections between these programs are also clearly visible in the next slide, which shows the interconnections of Equation Group. Equation Group's infrastructure includes more than 300 domains and 100 command and control servers located in various countries, particularly in the US, the UK, Italy, Germany, the Netherlands, Panama, Costa Rica, Malaysia, Colombia and the Czech Republic.

Kaspersky Lab has discovered that Equation Group interacted with some other cybergroups, particularly with the organizers of high-profile Stuxnet and Flame campaigns. In all likelihood, Equation Group shared zero-day exploits with their «colleagues». For example, in 2008 the Fanny worm used the same exploits that appeared in Stuxnet in June of 2009 and March of 2010, with one of these exploits being a module of Flame.

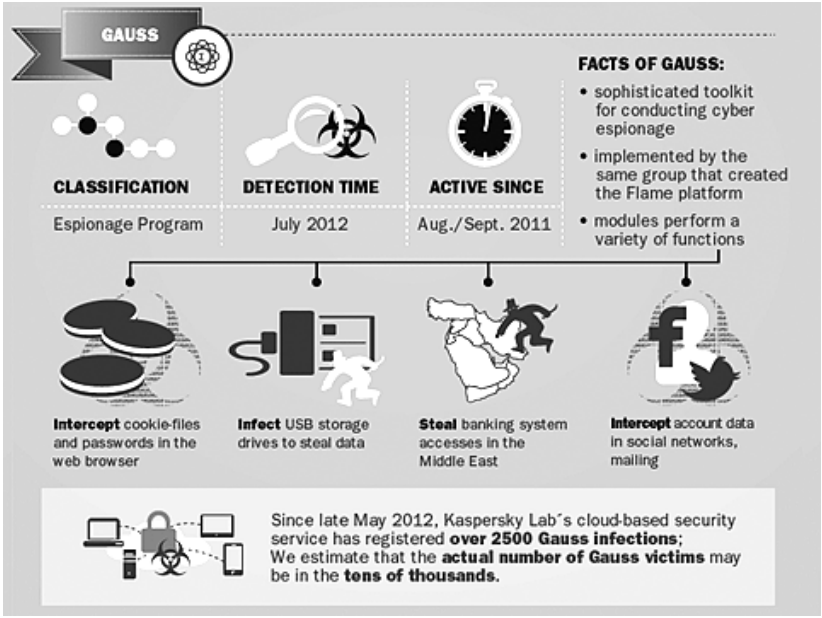
According to findings of our experts, at an early stage of infection Equation Group can use up to 10 exploits, but it is a rare practice to use more than three. Subsequently trying three different exploits, the group tries to get in, but if all three attempts are unsuccessful, the attackers retreat.



The next slides show the functionality of the two most interesting malicious programs, which we had to face. This is Flame, which is actually an advanced cyber-espionage toolkit — in it we found modules that have previously been used in Stuxnet.

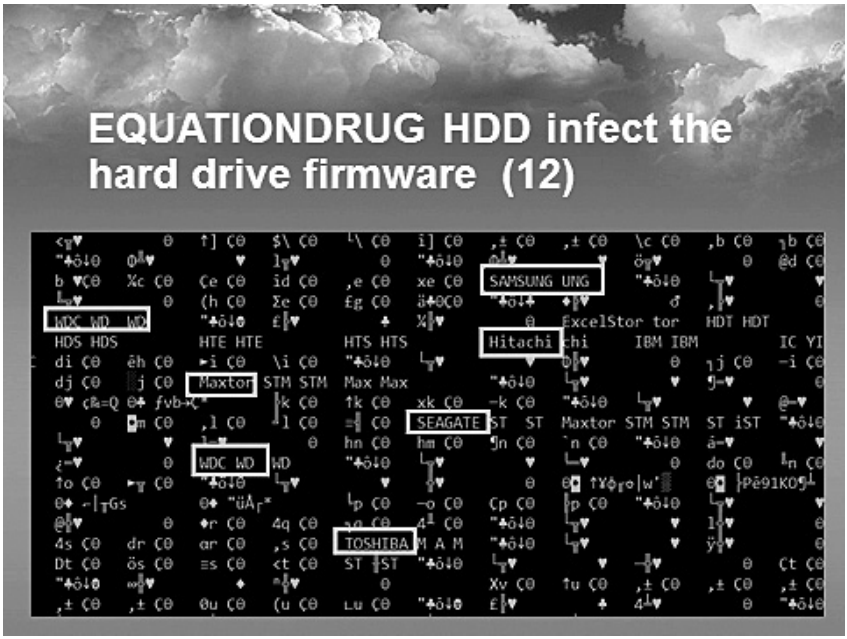


And the next is the Gauss malware, which additionally has an advanced functionality to spread through social networks. We have also discovered interesting capabilities for infection, storage and transmission of data through USB-flashcards.



Returning to the newer malware, the next slide is of interest, as it shows the names of companies that are the manufacturers of hard drives.

The inventory of Equation Group has lots of malware, and some of them are very innovative. For example, for the first time in its practice Kaspersky Lab has discovered modules that allow you to reprogram the hard drive firmware of 12 major manufacturers. It must be understood that in this way the attackers achieve two objectives: firstly, once introduced into the hard drive firmware, malware remains there indefinitely — it can be neither found nor removed: it cannot be removed even if the disk is formatted. Secondly, the attacker has the ability to create a «safe haven» in the form of a secret vault, where he can safely collect all the necessary information.



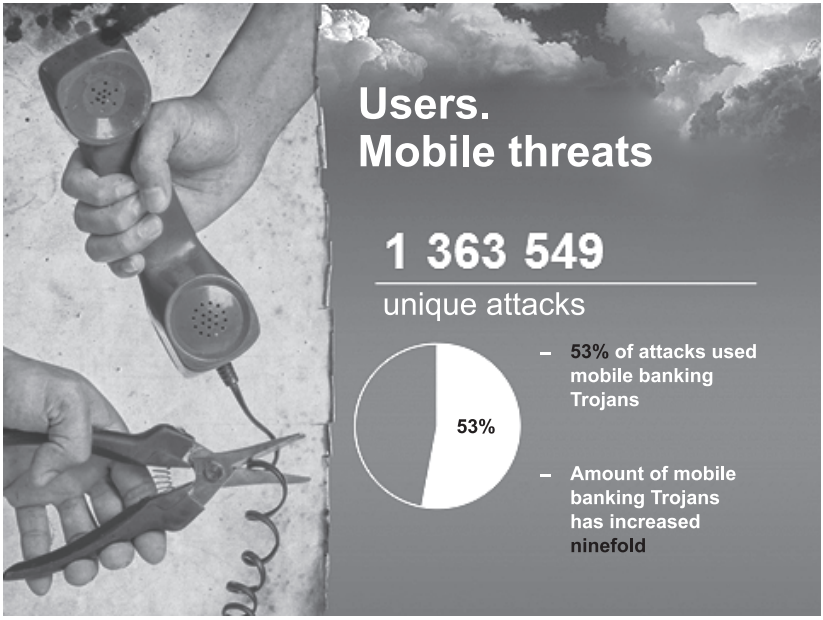
Next I would like to show the scope of operations of Equation Group and categories of infrastructure that have been infected. It is evident that Iran, Russia, Afghanistan and Pakistan were attacked the most. The computer systems of military, financial, government, diplomatic, energy, education, telecommunications, and aerospace structures faced the highest risk.

Here are several figures in continuation of cyberespionage topic. According to our data, in 2013–2014, the number of targeted attacks (APTs) has increased by 2.4 times and reached 4400 incidents.

The number of attacks on the business with the use of office applications has increased by 75%.

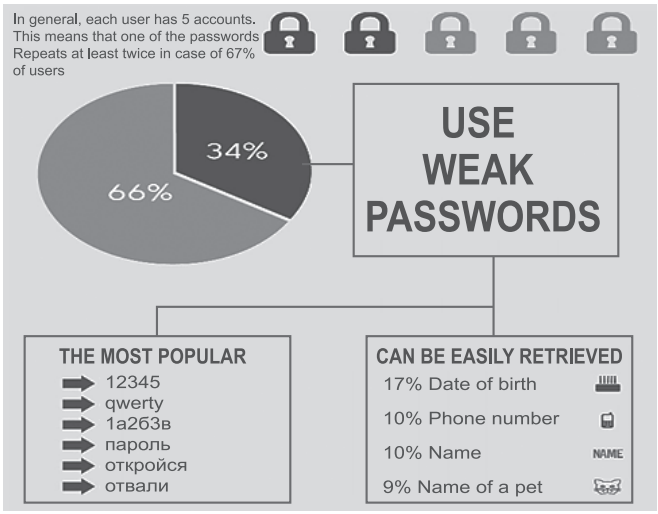
Cyberattack losses in Russia on average amount to 20 million rub. for big business and about 780 thousand rub. in medium and small companies. 1/3 of the companies have lost confidential data in these attacks. However one should take into account that most companies do not tend to disclose that they have become victims of cyberattacks and suffered losses. 91% of companies admitted that they would cease to do business with the financial institution that had become a victim of cyberattacks.

A few more figures. Users in Russia, financial threat: in 2013 — 6 million attacks, 2014 — 8 million attacks. Cellular threats: more than 1300 thousand unique attacks, 53% of which use mobile banking Trojans. Over the past year every fifth Android user has faced cyberthreats. The only positive thing that can be noted is that we see a 12% reduction of cellular spam.



In the last year due to personal data leaks and large amount of data obtained from infected computers, criminals came into possession of 1.26 million of Yandex mail accounts, 4.8 million of Mail.ru and more than 5 million of Gmail accounts.

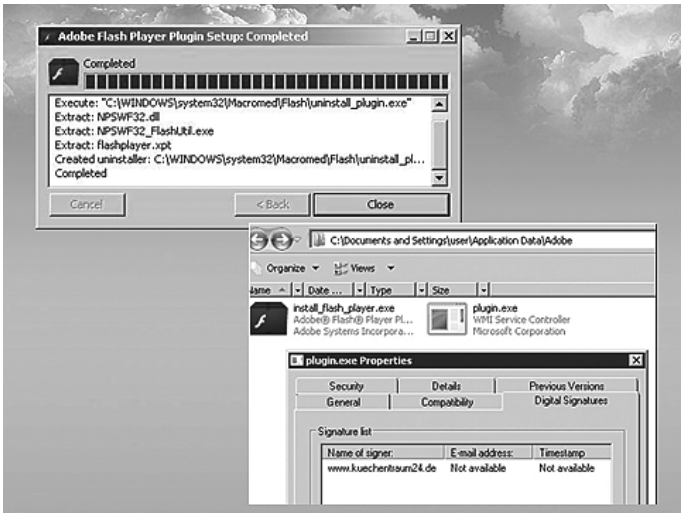
The analysis of leaks produced a list of commonly used passwords, led by 12345, qwerty, password date of birth or phone numbers of users, i.e., data that is readily available in social networks.



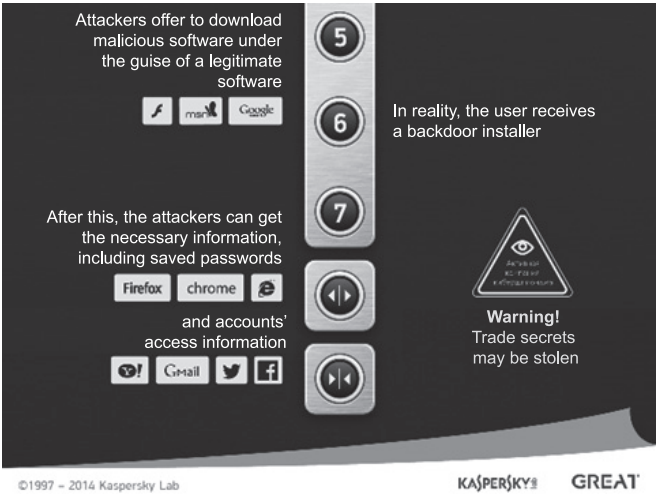
Another type of threat is associated with public Wi-Fi-networks. For example, in our hotel the access code consists of the name of the hotel and a year — seemingly the last time when it has been changed. According to our data, 26% of users connecting to the public Wi-Fi network log into social networks, and another 41% stores logins and

passwords from email and social networks accounts on their devices. Here is the scenario of a Darkhotel malware infection. After checking in at a hotel — upon connecting to public Wi-Fi network that was previously hacked or specially deployed by an attacker — user is requested to input a room number and a name.

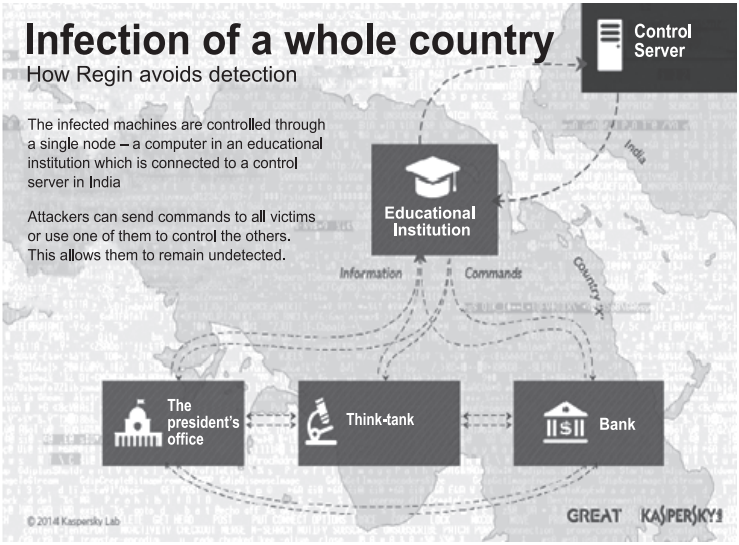
Next, you are prompted to install the «necessary» update, which includes executable malware, usually a backdoor installer. In this example, a normal run-time module of Adobe Flash Player has been used with added plugin.exe which contained a Trojan.



After this, the attackers gained access to all the information that was on the computer, including access to social network accounts, logins and passwords of mail services or access to bank accounts.



The scope of cybercriminal action of cannot be underestimated, in the next slide, I would like to show that there have been instances when the whole country was a victim of cyberattacks. In this example, threat came through an educational network, and in a short time government and financial services computers have been infected.



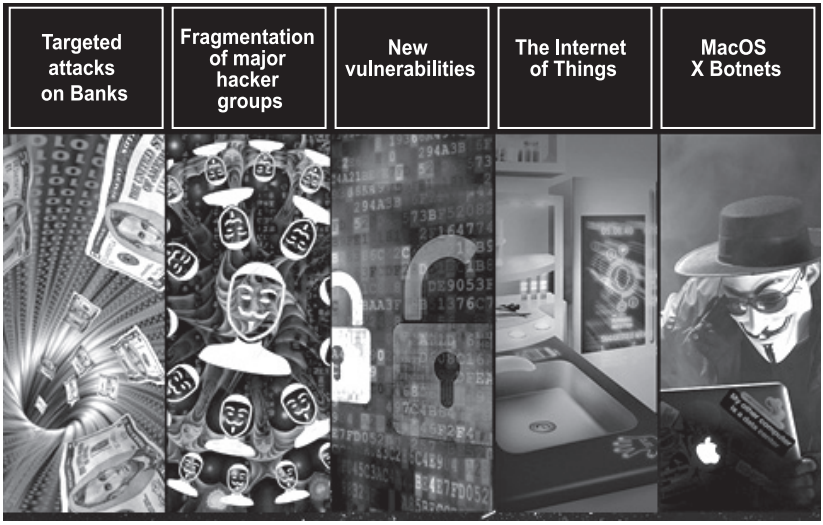
In conclusion, I would like to provide some tips, which, of course, are elementary and more focused on normal users rather than specialists in the field of information security:

Useful tips from Kaspersky Lab:

- Create a special card for online purchases and do not keep a large sum of money on it.
- Do not go to any websites via the links in emails, messages on social networks and chat rooms or by clicking the banner ads on dubious websites.
- Financial institutions never send out emails with request to: provide personal data in electronic communications; go to a website for authorization; or enter personal data in pop-up windows. Do not go to a website via the link provided on behalf of the banking institutions and payment systems.
- Do not click on any links sent by strangers.
- Avoid e-stores which are registered on free hosting servers.
- If the store's website raises doubts, use whois service to study data on lifetime of the domain that hosts the site and on its owner. Note the period for which the domain has been paid for.
- Enter the web address of the bank or payment system manually.
- Carefully study the URL of a webpage with input fields for confidential data. If an Internet address consists of a set of meaningless characters or URL looks suspicious, do not make a payment through this webpage.
- Check whether the transmission of your sensitive data uses encrypted connection. If the connection is secure, the website address should begin with https, and address bar or status bar should contain a closed padlock symbol.
- Avoid using online banking services or make online purchases in public places (Internet cafes, clubs, and libraries). Such machines can be infected with various spyware, key loggers, Internet traffic interceptors. Even if you use your own computer, but conduct banking operations through free public Wi-Fi network, there is a risk of: traffic interception by the administrator of the network; outsider wiretapping and worm attacks — especially if Wi-Fi network is not password protected.
- Always keep your operating system and anti-virus software updated. On your computer use anti-virus software with protection against phishing.

Vigilance and careful following of all the precautions can enable you to comfortably enjoy all the benefits that the Internet provides.

And a few words about major threats that will see further development in the near future: the forecast of Kaspersky Lab experts.



А.А.Стрельцов

Институт проблем информационной безопасности
МГУ имени М.В.Ломоносова

Адаптация международного права безопасности к информационному пространству

1. Актуальность проблемы адаптации международного права безопасности применительно к использованию ИКТ в качестве средства «силового» разрешения противоречий международной жизни является одной из задач государственной политики в области международной информационной безопасности[1].

Данная задача соответствует общей направленности резолюций Генеральной Ассамблеи ООН по вопросу о Достижениях в области информатизации в контексте международной безопасности (2010–2014), положений докладов Группы правительственных экспертов по достижениям в области информатизации в контексте международной безопасности (2010, 2013).

Необходимость решения задачи поддержана участниками международных конференций, организованных Международным Комитетом Красного Креста (Сан-Ремо — 2014, Москва — 2014, Санкт-Петербург — 2015).

По мнению экспертов, ситуация в области предотвращения конфликтов в киберпространстве характеризуется следующим.

С одной стороны, международное право безопасности применимо к информационному пространству (при этом учитывается, что источниками международного права являются: международные конвенции; международный обычай как доказательство всеобщей практики; общие принципы права, признанные цивилизованными народами; судебные решения и правовые доктрины — как вспомогательный материал). С другой стороны, единая позиция по порядку применения норм и принципов международного права к регулированию соответствующих международных отношений пока отсутствует.

2. Сложность решения проблемы применения международного права безопасности к киберпространству обусловлена следующими основными факторами.

---

[1] Основы государственной политики в области международной информационной безопасности на период до 2020 года. Утверждены Президентом Российской Федерации. 2013 г.

2.1. Отсутствие согласия между государствами — членами ООН по вопросу о предмете правового регулирования. Западные государства согласны обсуждать вопросы регулирования отношений в области использования ИКТ в качестве «силы», но не согласны обсуждать вопросы использования в качестве «силы» средств массовой информации и коммуникации.

2.2. Процессы злонамеренного использования ИКТ не наблюдаемы. Вследствие этого невозможно без использования специальных технических средств объективно установить ни факты вредоносного использования ИКТ, ни последствия такого использования ИКТ (величина и виды ущерба), ни субъектов, осуществляющих эти деяния. Общепринятые признаки вредоносного использования ИКТ, подлежащие регистрации техническими средствами, не определены. Международная система объективизации событий и атрибуции субъектов в киберпространстве отсутствует.

2.3. ИКТ не обладает признаками оружия. Это существенно затрудняет классификацию применения ИКТ в качестве «вооруженного нападения» или «вооруженных действий», порождающих, соответственно, правоотношения, связанные как с применением права на самооборону, так и с соблюдением норм международного гуманитарного права.

2.4. Правоприменение в области международной безопасности (в том числе в области ИКТ) осуществляется государствами самостоятельно с использованием национальных или региональных систем технических средств объективизации событий и атрибуции субъектов.

В рамках юрисдикции одного государства или группы дружественных государств правоприменение базируется на презумпции добросовестности действий лиц, осуществляющих оперативно-следственные мероприятия по фактам злонамеренного использования ИКТ.

При взаимодействии государств, не связанных отношениями доверия, презумпция добросовестности невозможна ввиду того, что технологический потенциал многих государств достаточен для того, чтобы фальсифицировать данные о почти любых событиях и субъектах киберпространства.

2.5. В международном праве отсутствуют механизмы закрепления адресного пространства применения ИКТ к национальным границам. В настоящее время функции распределения IP-адресов выполняются в основном негосударственными организациями,

не являющимися субъектами международных публичных отношений.

Это создает дополнительные сложности при определении в киберпространстве границ театров военных действий, нейтральных государств, обозначении объектов и лиц, охраняемых международным публичным правом.

2.6. Учитывая, что ни одно государство не имеет международных обязательств в области обеспечения безопасности киберпространства, представляется затруднительным определение границ национального суверенитета и юрисдикции государств. Данный вопрос особенно важен в свете существующей практики государств рассматривать обеспечение безопасности киберпространства в качестве одной из составляющих национальной безопасности.

3. В настоящее время известно два методических подхода к решению рассматриваемой проблемы.

3.1. Первый поход базируется на развития общих принципов права. Данный подход активно развивает группа специалистов, работающих по заказу Центра кибероборонь НАТО в Таллинне (Эстония). По заданию этого Центра международная группа экспертов (юристов и специалистов в области информатики) подготовила так называемое Таллиннское руководство по киберконфликтам[2], которое часто позиционируется специалистами западных государств как возможная основа для подготовки универсальной международной конвенции.

Можно сформулировать несколько замечаний по существу предложенного в Руководстве подхода.

Как отмечено в Предисловии к Руководству, методологически материал базируется на проекте Конвенции о международной правовой ответственности государств за нарушение международного права, который рассматривается в качестве источника международного права, хотя всего лишь был обсужден и принят к сведению Генеральной Ассамблеей ООН[3] (2001). В проекте Конвенции одним из центральных положений является право каждого государства или группы государств в рамках их суверенитета и юрисдикции самостоятельно осуществлять:

- трактовку наблюдаемых ими событий в киберпространстве в качестве опасных для национальной информационной инфраструктуры;

---

[2] Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual). M.Schmitt et al. eds. Cambridge University Press, forthcoming 2013.

[3] Ответственность государств за международно-противоправные деяния. Резолюция Генеральной Ассамблеи ООН 56/83 от 21 декабря 2001.

- классификацию этих событий как соответствующих нормам международного права или как международно-противоправные деяния;
- принятие решений о том, какое государство ответственно за событие, которое классифицируется как международно-противоправное деяние;
- применение к государству, определенному в качестве ответственного за опасное нарушение международного права, неких контрмер.

Представляется, что при отсутствии механизма объективизации событий в киберпространстве и атрибуции субъектов таких действий, а также общепринятой трактовки понятия «международно-противоправные деяния государств» и перечня таких деяний применение данного положения проекта Конвенции с неизбежностью увеличивает опасность провоцирования вооруженного конфликта между государствами.

К аналогичным последствиям приведет применение рекомендации Руководства об отсутствии необходимости учета признака «вооруженного» нападения при рассмотрении «компьютерной операции» против государства — члена ООН. Отказ от учета данного признака размывает жесткие границы правомерного поведения государств в области применения права на индивидуальную и коллективную самооборону, закреплённые Статьей 51 Устава ООН, и, как следствие, — приводит к увеличению опасности возникновения международных конфликтов, спровоцированных возможно ошибочными предположениями о существовании факта злонамеренного использования ИКТ и о наступлении в связи с этим последствий, превышающих пороговые значения для возникновения предусмотренных международными договорами правоотношений по поводу угрозы силой или ее применения против территориальной целостности или политической независимости государства-жертвы, либо «вооруженного нападения» на него.

Международная группа экспертов, подготовивших Таллиннское руководство, оставила без внимания то обстоятельство, что в рамках существующих международных конвенций ни одно государство не имеет каких бы то ни было обязательств по обеспечению устойчивости функционирования сети Интернет (вряд ли таковыми можно считать обязательства организации ICAAN, которая записала себе в уставные документы обеспечение безопасности управления системой DNS). Одновременно, предполагается, что такие обязательства по отношению к национальным сегментам данной сети (границы не определены), как и ответ-

ственность за их выполнение вытекают из общих принципов права. Данные обстоятельства при определенных обстоятельствах также могут спровоцировать возникновение международного конфликта.

Изложенное позволяет сделать вывод о том, что реализация данного подхода может нанести ущерб международной безопасности, так как, по существу, приводит к деградации механизма предупреждения конфликтов, закреплённого Уставом ООН, и не способствует достижению одной из главных целей ООН — «избавить грядущие поколения от бедствий войны» (Преамбула Устава ООН).

3.2. Второй методический подход к решению рассматриваемой проблемы базируется на использовании потенциала прогрессивного развития позитивного права — Устава ООН, международных конвенций и договоров в области международной безопасности.

В его основу предлагается положить концепцию «неявного оружия», определяющую условия возможного рассмотрения ИКТ в качестве оружия.

Данная концепция базируется на прецеденте, созданном резолюциями Совета Безопасности ООН[4] по результатам обсуждения трагических событий, произошедших в США 11 сентября 2001 г. Как известно, в рамках этих событий была осуществлена атака международных террористов на гражданские и военные объекты с использованием гражданских самолетов в качестве средств поражения. Совет Безопасности ООН не возражал против применения США в соответствии со ст. 51 Устава ООН «неотъемлемого права государства на индивидуальную и коллективную самооборону» и, соответственно, — применения вооруженной силы против Афганистана в рамках объявленной глобальной войны с международным терроризмом.

Таким образом, упомянутыми решениями СБ ООН введена в международную практику концепция «неявного оружия». Ее существо заключается в следующем. Любое невоенное устройство или механизм может приобрести свойства оружия, если нарушение нормального функционирования такого устройства или механизма (в том числе посредством использования ИКТ) может быть использовано для нанесения поражения живой силы и военной техники. В этом случае нападение на территорию государства с использованием таких устройств или механизмов может квалифицироваться как «вооруженное нападение».

---

[4] Резолюции Совета Безопасности ООН №1368 от 12 сентября 2001 г. и №1373 от 28 сентября 2001 г.

Принятие концепции «неявного оружия» в качестве основы для выявления признаков использования государствами ИКТ в качестве «применения силы» и «вооруженного нападения» позволяет выделить следующие основные направления адаптации международного права безопасности:

- уточнение терминологии международного права предотвращения конфликтов применительно к киберпространству (правила ответственного поведения государств в киберпространстве;
- мирное разрешение международных споров, связанных с фактами злонамеренного использования ИКТ;
- обнаружение атак с использованием ИКТ, оценка последствий, квалификация атак, способы разрешения международного спора);
- прогрессивное развитие принципов и норм международного гуманитарного права к условиям ведения военных действий с использованием ИКТ в качестве «неявного оружия» (делимитация национальных границ в киберпространстве; обозначение объектов, защищаемых международным гуманитарным правом; объективизация опасных событий, связанных со злонамеренным использованием ИКТ;
- атрибуция государств, инициировавших злонамеренное использование ИКТ);
- развитие принципов и норм международного права прав человека применительно к условиям ведения военных действий с использованием ИКТ;
- развитие норм международного процедурного права применительно к случаям злонамеренного использования ИКТ для разрешения международных споров.

Адаптация норм международного права безопасности к киберпространству и закрепление правовых новаций в международных правовых актах позволит заложить основы международного правового режима кибербезопасности.

Отдельным вопросом, требующим рассмотрения в рамках адаптации международного права предотвращения конфликтов и международного гуманитарного права к киберпространству является форма закрепления предлагаемых правовых новаций.

Таким образом, при реализации подхода, основанного на концепции «неявного оружия», оказывается возможным не только существенно снизить опасность возникновения международных конфликтов, спровоцированных вредоносным использованием ИКТ, но и создать условия для реализации положений ст. 2 (3) Устава ООН по мирному разрешению международных споров.

A.A.Streltsov
Moscow State University
Institute of Information Security Issues

Adaptation of international security law to information space

1. The importance of the issue of international security law adaptation with regard to use of ICTs as means of «coercive» solution of tensions in international relations is one of the aspects of the nation-states' policy in the field of international information security[1].

This is consistent with the general focus of the UN General Assembly resolutions on the Developments in the field of information and telecommunications in the context of international security (2010–2014), and the reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2010, 2013).

The need to find solutions to the problem was supported by the participants of international conferences organized by the International Committee of the Red Cross (San Remo — 2014, Moscow — 2014, St. Petersburg — 2015).

According to experts, the situation in the field of conflict prevention in cyberspace is characterized by the following.

On the one hand, international security law is applicable to information space (it is taken into account that the sources of international law are: international conventions; international custom, as evidence of a general practice; general principles of the law recognized by civilized nations; judicial decisions and legal doctrines — as auxiliary material). On the other hand, there is no consensus on the administration of the rules and principles of international law relevant to regulation of corresponding international relations.

2. The complexity of finding the solution to the issue of international security law application to cyberspace is determined by the following factors.

2.1. There is a lack of agreement between the member-states of the United Nations on the subject of legal regulation. The Western states are willing to discuss issues of regulation of relations with regard to

[1] Основы государственной политики в области международной информационной безопасности на период до 2020 года. Утверждены Президентом Российской Федерации. 2013 г.

the use of ICTs as a «force», but do not agree to discuss their use as a «power» of the media and communications.

2.2. The processes of malicious use of ICTs are not observable. As a consequence, without the use of special technical means it is impossible to objectively ascertain neither the facts or malicious use of ICTs, nor the consequences of the use of ICTs (the extent and type of damage) nor the entities engaged in these acts. Common attributes of malicious use of ICTs to be recorded by technical means are not defined. There is no international system of objectification of events and attribution of subjects in cyberspace.

2.3. ICTs have no attributes of weapons. This makes it significantly more difficult to classify the use of ICTs as an «armed attack» or «hostilities» that respectively bring about legal relationships associated with both the application of the right to self-defense, and compliance with international humanitarian law.

2.4. Enforcement in the field of international security (including the sphere of ICTs) is carried out by nation-states discretionary with the use of national or regional technical means of objectification of events and attribution of subjects.

Within the jurisdiction of one nation-state or a group of friendly nations enforcement is based on presumption of fairness of the individuals (and their actions) engaged in the operative investigative measures over the facts of malicious use of ICTs.

Considering interactions between the nations that are not in relations of mutual trust, presumption of fairness is impossible due to the fact that many nation-states have sufficient technological capabilities to falsify data on almost all events and subjects of cyberspace.

2.5. International law doesn't provide for frameworks to bind the address space where ICTs are applied to national borders. Presently, the functions of IP-addresses distribution are largely performed by non-governmental organizations, who are not the subjects of international public interactions.

This creates additional difficulties when defining the boundaries of battle grounds and neutral states, designation of objects and persons protected by international public law in cyberspace.

2.6. Considering the fact that no nation-state has international obligations in the field of cyberspace security, it is difficult to define the boundaries of national sovereignty and jurisdiction of nation-states. This issue is particularly important in the light of the current practice, when nation-states consider cyberspace security as an element of national security.

3. Presently there are two methodological approaches to solving the problem.

3.1. The first approach is based on the development of general principles of law. This approach is being actively pursued by a team of specialists who have been commissioned by the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn (Estonia). As assigned by this Centre, an international group of experts (lawyers and experts in the field of computer science) has developed a so-called Tallinn Manual on the International Law Applicable to Cyber Warfare[2], which is often promoted by specialists of Western countries as a possible framework for the preparation of a universal international convention.

One can formulate a few remarks on the essence of approach proposed by the Manual.

As noted in the Preface to the Manual, the proceedings are methodologically based on the draft Convention on Responsibility of States for internationally wrongful acts, which is treated as a source of international law, although it has only been discussed and noted by the United Nations General Assembly (2001)[3]. One of the central provisions of the draft Convention is the right of every State or group of States to carry out within their own sovereignty and jurisdiction:

- interpretation of observed events in cyberspace as hazardous to the national information infrastructure;
- classification of these events as meeting the norms of international law or as internationally wrongful acts;
- decisions about what country is responsible for the event, which is classified as an internationally wrongful act;
- countermeasures against the country that is ascertained to be responsible for a dangerous violation of international law.

It appears that without a framework for objectification of events in cyberspace and attribution of the subjects of such actions, as well as in the absence of generally accepted interpretation of the term «internationally wrongful acts of States» and a list of such acts, the application of provisions of the draft Convention inevitably increases the risk of provoking an armed conflict between nation-states.

Similar consequences will follow the implementation of recommendation of the Manual that it is not necessary to take into account an attribute of an «armed» attack when investigating a «computer opera-

---

[2] Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual). M.Schmitt et al. eds. Cambridge University Press, forthcoming 2013.

[3] Ответственность государств за международно-противоправные деяния. Резолюция Генеральной Ассамблеи ООН A/RES/56/83 от 21 декабря 2001.

tion» against a member-state of the UN. The removal of this attribute blurs the rigid boundaries of lawful conduct of nation-states in the application of the right of individual and collective self-defense, enshrined in Article 51 of the UN Charter. As a consequence, this leads to an increase of risk of international conflict, which may be provoked by possible erroneous assumptions about the existence of the fact of malicious use of ICTs and ensuing of relevant consequences that exceed the thresholds for the emergence of relations under international treaties about an «armed attack» or the threat or use of force against the territorial integrity or political independence of the victim nation-state.

The international team of experts which prepared the Tallinn Manual disregarded the fact that under existing international conventions no nation-state has any obligations whatsoever to ensure the sustainability of the Internet (we can hardly consider as such the obligations of ICAAN, which in its statutory documents has self-assigned the security of DNS to itself). At the same time, it is assumed that such obligations with regard to the national segment of the network (the boundaries are not defined), as well as responsibility for their fulfillment are derived from the general principles of the law. Under certain circumstances these aspects can also provoke an international conflict.

The foregoing leads to a conclusion that the implementation of this approach can be detrimental to international security, as, in fact, leads to degradation of conflict prevention mechanisms enshrined in the UN Charter, and does not contribute to one of the main objectives of the United Nations — «to save succeeding generations from the scourge of war» (Preamble of the UN Charter).

3.2. The second methodological approach to solution of the problem is based on exploiting the potential for progressive development of positive law — the UN Charter, international conventions and treaties in the field of international security.

It is based on proposed concept of «implicit weapons», which determines the conditions for a possible consideration of ICTs as a weapon.

This concept is found upon the precedent created by the UN Security Council resolutions[4] based on discussion of the tragic events of September 11, 2001. It is known, that as part of these events international terrorists attacked civilian and military targets by use of civil aircraft

[4] Резолюции Совета Безопасности ООН №1368 от 12 сентября 2001 г. и №1373 от 28 сентября 2001 г.

as weapons of destruction. The UN Security Council did not object to exercise of «inherent right of individual or collective self-defence» by the United States in accordance with Article 51 of the UN Charter and, therefore, — to the use of armed force against Afghanistan in the framework of declared global war on international terrorism.

Thus, the above mentioned UN Security Council resolutions introduced the concept of «implicit weapons» in international practice. Its essence includes the following aspects. Any non-military device or mechanism can acquire the properties of weapons, if disruption of normal functioning of such device or mechanism (including through the use of ICTs) can be used to injure personnel and/or damage military equipment. In this case, attack on the territory of a nation-state by the use of such devices or machines can be qualified as an «armed attack».

The adoption of «implicit weapons» concept as a basis for identification of the use of ICTs by the nation-states as the «use of force» and «armed attack» allows us to highlight these main areas of adaptation of international security law:

- clarification of the terminology of international law of conflict prevention with regard to cyberspace (rules of responsible behavior of nation-states in cyberspace);
- peaceful resolution of international disputes related to instances of malicious use of ICTs;
- detection of attacks with the use of ICTs (impact assessment, subsumption of attacks, methods of settling international disputes);
- progressive development of principles and norms of international humanitarian law with regard to conduct of hostilities with the use of ICTs as «implicit weapons» (delimitation of national borders in cyberspace; designation of objects protected under international humanitarian law; objectification of hazardous events associated with malicious use of ICTs; attribution of nation-states that initiated the malicious use of ICTs);
- development of principles and norms of international human rights law with regard to the aspects of military activities with the use of ICTs;
- development of international procedural law with regard to cases of malicious use of ICTs for settlement of international disputes.

The adaptation of international security law to cyberspace and consolidation of the legal developments in international legal instruments would lay the foundations of international legal framework for cybersecurity.

An actual form of consolidation for proposed legal developments is a separate issue to be addressed in the framework of adaptation of international humanitarian law and international law of conflict prevention to cyberspace.

Thus, the implementation of an approach based on «implicit weapons» concept makes it possible not only to significantly reduce the risk of an international conflict provoked by malicious use of ICTs, but also to create conditions for the implementation of the UN Charter Article 2 (3) provisions for peaceful settlement of international disputes.

Маурицио Мартеллини

Центр международной безопасности Университета Инсубрия (Италия)

Клэй Уилсон

Система Американских государственных университетов

Следующее поколение кампаний с использованием кибероружия и риск Армагеддона в киберпространстве

Кибератака является привлекательным вариантом действий в ходе войны. Государства могут счесть целесообразным оказывать влияние или принуждение на другие страны посредством военных кампаний в киберпространстве, пользуясь анонимностью и возможностью отрицания. В недавнем прошлом было несколько раз показано, что использование вредоносного программного кода может вызвать физическое разрушение критически важных инфраструктур путем манипуляций с промышленными системами управления. Кибератаки также свели к минимуму необходимость рисковать личным составом или дорогостоящим оборудованием. Вредоносный код также является многоразовым, представляя собой практически бездонную обойму для будущих атак. Однако подобные преимущества «чистой» войны также имеют темную сторону. Учитывая удобство, быстроту и снижение потерь личного состава, также существует соблазн использовать кибератаки часто, и, возможно, оказывать предпочтение им вместо участия в длительных или тщетных переговорах. Кроме того, экстремистские группы могут оказаться в состоянии приобрести копии вредоносного программного кода и анонимно использовать его против невоенных целей.

Устав ООН предусматривает руководящие принципы для обоснования ответных действий на кибератаки, являющиеся применением силы. Они приведены в статье 2 (4) — разрушительные действия, подходящие под определение «применение силы», и в статье 51 — разрушительные действия, подходящие под определение «вооруженного нападения», несущие угрозу государственному суверенитету. Однако большинство кибератак последних лет не смогли нарушить способность государств осуществлять свой суверенитет. Кроме того, в некоторых странах существуют правовые полномочия, обеспечивающие руководящие принципы

проведения наступательных кибератак. В Соединенных Штатах, такие полномочия содержатся в:

- *Разделе 10 Свода законов США* — где указано, что военные операции не требуют предварительных письменных решений до осуществления действий. Однако будет сложно отрицать проведение операций, осуществляемых согласно содержащимся в этом разделе полномочиям.
- *Разделе 50 Свода законов США*, посвященному проведению тайных операций США. Используя содержащиеся в разделе полномочия, Президент должен предоставить письменное свидетельство, что операция осуществляется для реализации определенной задачи внешней политики и национальной безопасности. Когда неясно, является ли кибератака применением силы в соответствии с Уставом ООН, то Раздел 50 делает возможным тайное проведение и отрицаемость действий.

Сообщения СМИ свидетельствуют о том, что кибератаки становятся все более изощренными и более скрытными. В случаях повреждения физического оборудования существует тенденция сравнивать вредоносный программный код с оружием. Но что такое оружие, и в каких случаях кибератаки на законных основаниях можно назвать кибероружием?

В США каждый вид вооруженных сил имеет закрепленное определение, что представляет собой оружие. В то же время, оружие должно также отвечать международным правовым стандартам. Статья 22 Гаагской и Статья 36 Женевской конвенций говорят о том что «средство», именуемое оружием, не может быть использовано вооруженными силами до проведения правовой экспертизы. Гаагская и Женевские конвенции предназначены для защиты гражданского населения от излишних страданий во время войны. При этом можно продемонстрировать, что многие кибератаки также оказали непредсказуемый побочный эффект на гражданское население. «Таллинское Руководство по применимости международного права к вооруженным действиям в киберпространстве» было разработано после того, как Эстония подверглась разрушительным кибератаким в 2007 году. Руководство определяет кибероружие как «киберсредства ведения войны», которые созданы или используются для причинения вреда лицам или объектам. Это определение оружия не включает в себя уничтожение данных, если нет прямой связи с нанесением ущерба или работоспособностью компьютерной системы. Таким образом, если посредством кибератаки осуществлено умышленное повреждение или намеренное нарушение работоспособности

компьютеров, то мы имеем дело с кибероружием. Однако, как показал реверс-инжиниринг и анализ недавних кибератак высокого уровня, существует несколько дополнительных характеристик, которые также должны быть учтены при формулировании более точного определения кибероружия.

В недавних сообщениях СМИ несколько примеров высокотехнологичных вредоносных кодов были названы кибероружием. В этих сообщениях были приведены результаты обширных исследований вредоносного кода под именами Flame, Duqu и Stuxnet. Сообщается, что эти три вредоносные киберпрограммы были использованы как часть комбинированной многолетней киберкампании, направленной на нарушение функционирования определенных объектов ядерной промышленности в Иране. Возможно, что эта вредоносная киберкампания тайно проводилась на главных иранских объектах по крайней мере с 2006 по 2010 год, прежде чем была обнаружена сотрудниками служб безопасности, работающими за пределами Ирана. Следовательно, в дополнение к определению, данному в Таллинском руководстве, существующее поколение кибероружия может также потребовать учета следующих характеристик:

- скрытность, которая позволяет вредоносным программам тайно функционировать в течение длительных периодов времени;
- использование ряда вредоносных программ, которые сочетают в себе такие различные задачи, как шпионаж, хищение данных или саботаж;
- специальные технологии, которые позволяют вредоносному коду обойти или обмануть защитную технологию управления кибербезопасностью.

Специальная технология, позволяющая обойти или обмануть системы кибербезопасности, в том числе те, которые должны защищать такие сверхсекретные промышленные объекты, как АЭС в Иране, называется атака «нулевого дня». Она представляет собой определенный вредоносный код, выполняемый перед основной вредоносной программой, и предназначена для использования уязвимости, которая является новой и неизвестной в целевой системе. Атака нулевого дня способна полностью или временно вывести из строя систему управления кибербезопасностью, и таким образом открыть целевую компьютерную систему для внедрения и начала работы основной вредоносной программы. Многие высококвалифицированные хакеры усердно работают над обнаружением новых уязвимостей в системах, которые позволяют создавать новые атаки «нулевого дня». Мотивацией

для этих хакеров является то, что атаки «нулевого дня» можно дорого продать государствам или экстремистам. Атаки «нулевого дня», обнаруженные и разработанные высококвалифицированными хакерами, являются важной составляющей существующего поколения кибероружия.

Последней характеристикой, которая позволяет успешно использовать вредоносный код в качестве кибероружия, является то, что можно описать как «доскональное знание» целевых промышленных систем управления гражданской и/или военной техники. Хакеры, создавшие атаки «нулевого дня», которые были использованы в кибероружии, примененном в ходе кампании против Ирана, по-видимому, имели очень хорошее понимание о целевом промышленном оборудовании. Эти узкоспециализированные знания разработчика, используемые в создании различных вредоносных кодов для шпионажа и саботажа, являются тем, что делает существующее поколение кампаний кибероружия таким эффективным.

Однако у существующего поколения кампаний кибероружия также могут быть проблемы. Есть вероятность, что кибероружие выйдет из-под контроля. Например, Stuxnet, как сообщается, несколько раз обновлялся для расширения функциональности, и, в конце концов, вредоносный код вышел за пределы иранского предприятия по обогащению урана. Образцы Stuxnet были обнаружены во многих странах за пределами Ирана. Тем не менее, другие объекты не были повреждены, поскольку вредоносный код в Stuxnet был разработан для нападения только на специализированное оборудование на ядерном объекте в Иране. В будущем кибероружие, разработанное менее тщательно чем Stuxnet, также может неожиданно распространиться и, возможно, стать причиной побочного ущерба на других объектах.

В будущем среда и возможности для осуществления кибератак будут расширяться. В прошлом целями были промышленные системы управления критически важных инфраструктур, таких, как нефте- и газопроводы, а также гражданские электростанции. По мере того, как в Интернете будет появляться больше подробной «доскональной» информации, вероятно, что в перспективе целями станут сложные военные объекты и системы вооружения, в том числе больше примеров нападений на ядерные объекты или системы командования, управления и связи (C3) плюс компьютерные системы (C4), и системы противоракетной обороны (как ракеты земля-воздух). Например, советский зенитно-ракетный комплекс БУК с помощью которого, как сообщается, в

июле 2014 года был сбит рейс Malaysia Airlines 17, и погибло 298 человек, является тщательно разработанной системой, но может иметь уязвимости, и не обладает способностью самостоятельно отличить гражданские цели от военных. К сожалению, детальная информация о зенитно-ракетной системе БУК доступна в Интернете. Техническая документация для этой системы, а также для нескольких российских ракетных пусковых установок может быть загружена из Интернета в виде достоверного программного тренажера, что позволяет любому изучать и практиковаться в базовом режиме работы нескольких советских зенитно-ракетных пусковых установок.

Другим примером роста уязвимости сложной военной техники является то, что Научный совет Министерства обороны США передал Пентагону секретный список систем боевого оружия, документация по которым была украдена в результате кибершпионажа. Список включает в себя проекты продвинутой ракетной системы Patriot, известной как PAC-3 (см. Washington Post, Эллен Накашима, от 27 мая 2013 года). В отдельном докладе, который также можно найти в Интернете, приведены результаты анализа уязвимостей в программном обеспечении системы национальной противоракетной обороны, в том числе ракетной системы Patriot PAC-3 («Using Genetic Algorithms to Aid in a Vulnerability Analysis of National Missile Defense Simulation Software» — JDMS, Volume 1, Issue 4, October 2004 Page 215–223, http://www.scs.org/pubs/jdms/vol1num4/imsand.pdf).

Подводя итоги, кибератаки становятся все более изощренными, и в случае, если имеются следующие характеристики — а) использование атак нулевого дня для обхода технологий кибербезопасности, б) проведение кампаний с координированным использованием различных вредоносных программ, и в) использование скрытности при долговременном проведении вредоносных операций для шпионажа или саботажа — мы можем иметь дело с кибероружием. Правильное проведение атрибуции является затруднительным, а технологии, используемые для обеспечения кибербезопасности, становятся все менее адекватными при расширении задач защиты от кибероружия. Таким образом, классическая теория сдерживания, разработанная для ядерного оружия, не работает для кибероружия. Кроме того, есть вероятность, что кибероружие выйдет из-под контроля. В будущем кибероружие, разработанное менее тщательно, чем Stuxnet, также может неожиданно распространиться и, возможно, вызвать побочный ущерб. В довершение ко всему, исследование примеров существующего

поколения кибероружия также показало, что подробные и доскональные знания о целевой системе способствуют успеху диверсионной киберкампании. По мере того, как в Интернете (возможно, посредством кибершпионажа) появляется больше информации, описывающей детальные подробности и возможные уязвимости современного оборудования и сооружений, в том числе военной техники, они также могут стать целями для будущих поколений кибероружия.

Есть много политических вопросов, связанных с кибербезопасностью и кибервойнами, которые заслуживают дальнейшего исследования:

- Какие стратегии могут помочь в уменьшении/регулировании глобального распространения вредоносных атак нулевого дня/вредоносного программного обеспечения, предназначенных для ведения кибервойны?
- Будущие наступательные кампании, скорее всего, уже развернуты и в настоящее время работают. Как можно обнаружить и изолировать их?
- Существует ли и что собой представляет правомерность в рамках международного (и гуманитарного) права в вопросе использования/угрозы применения ядерного оружия в качестве возмездия против использования кибероружия?
- Возможно ли создание механизма контроля над кибервооружениями? Если да, то сколько времени это займет, принимая во внимание что система контроля над ядерным оружием создавалась десятилетиями?
- Является ли СБ ООН по-прежнему предпочтительным учреждением для осуществления глобального контроля над кибервооружениями?
- Если да, должны ли постоянные члены СБ ООН открыто раскрыть все кибероружие, чтобы избежать Армагеддона в киберпространстве?

Prof. Maurizio Martellini
Insubria Center on International Security (Italy)

Dr. Clay Wilson
American Public University System

Next Generation Cyber Weapon Campaigns and Risks of a Cybergeddon

Cyberattack is an attractive option for warfare. Nation states may find it advantageous to influence or coerce other countries while taking advantage of anonymity and deniability through military campaigns that operate in cyberspace. It has been demonstrated several times in the recent past that the use of malicious cyber code can cause physical disruption of critical infrastructures through manipulation of industrial control systems (ICS). Cyberattacks also minimize the need to risk military personnel or costly equipment. Malicious code is also reusable, offering a practically bottomless magazine for future attacks. However, such advantages for "clean" warfare also have a darker side. With all the conveniences, swiftness, and reduced loss of personnel, there is also the temptation to use cyberattacks frequently, and perhaps favor using them instead of engaging in prolonged or frustrating negotiations. In addition, extremist groups may be able to acquire copies of malicious cyber code to use anonymously against targets that are non-military.

The UN Charter provides guidelines for justifying a response to a cyberattack that represents a use of force. These are found in Article 2(4) — disruption through meeting the definition for "use of force", and in Article 51 — disruption through meeting the definition for an "armed attack" that threatens to disrupt national sovereignty. However, most recent cyberattacks have fallen short of disrupting the ability of a nation state to exercise its sovereignty. Also, in some countries, there are legal authorities that provide guidelines for launching offensive cyberattacks. In the United States, the authorities for offensive cyberattacks are found in:

- *Title10 USC* — where military operations do not require written findings in advance of taking action. However, operations under this authority may not offer easy deniability of cyberattack action.
- *Title 50 USC* — where the US engages in covert actions. Under this authority, the President must make a written finding that the action

supports an identifiable foreign policy and national security objective. When it is uncertain whether a cyberattack might amount to a use of force under the UN Charter, then Title 50 enables secrecy and deniability of action.

Recent news reports show that cyberattacks are becoming more sophisticated and more stealthy. When damage to physical equipment also occurs, there is a tendency to start comparing malicious cyber code to weaponry. But, what is a weapon, and when are cyberattacks legitimately called Cyber Weapons?

In the US, every military service has a written definition for what comprises a weapon. However, a weapon must also meet international legal standards. The Hague Article 22 and Geneva Article 36 describe how a "capability" that is called a weapon cannot be used by the military until after a legal review. The Hague and Geneva Conventions are intended to protect the civilian population from unnecessary suffering during a war. However, it can be shown that many cyberattacks have also had unpredictable collateral effects on the civilian population. The "Tallinin Manual on International Law Applicable to Cyber Warfare" was developed after highly-disruptive cyberattacks were directed against Estonia in 2007. This Manual defines a cyber weapon as a "cyber means of warfare" that is capable, by design or intent, of causing injury to persons or objects. This definition of a weapon excludes the destruction of data, unless there is direct connection to injury, or the functionality of a computer system. So, if there is intentional injury, or if computer functionality is intentionally disrupted through a cyberattack, then we experiencing a cyber weapon. However, reverse-engineering and analysis of recent sophisticated cyberattacks has shown there are several additional characteristics that must also be present to develop a more accurate definition for a cyber weapon.

Recent news reports have labeled several examples of highly-sophisticated malicious code as cyber weapons. These reports have included results of extensive studies of malicious code with names such as Flame, Duqu, and Stuxnet. These three examples of malicious cyber programs were reportedly used as part of a combined multi-year cyberattack campaign intended to disrupt the operations of specific nuclear processing facilities in Iran. This malicious cyber campaign may have been secretly ongoing inside the Iranian top facilities from at least 2006 through 2010 before being discovered by security personnel working outside Iran. So, in addition to the definitions in the Tallinin Manual, the current generation of cyber weapons may also require these following characteristics:

- stealth that enables malicious programs to operate secretly over extended time periods
- multiple malicious programs that combine different missions such as espionage, data theft, or sabotage
- a special technology to enable the malicious code to bypass or fool protective cybersecurity control technology.

The special technology to bypass or fool cybersecurity controls, including those that supposed to protect top-secret industrial facilities such as the nuclear plant in Iran, is called Zero Day Exploits. A Zero-Day Exploit (ZDE) is a specific malicious code prefixed onto a larger malicious program payload, and is designed to take advantage of a vulnerability that is new and unknown in the targeted system. A ZDE is able to defeat or temporarily suspend the operation of cyber security controls, and thus open a targeted computer system so that a malicious payload can enter and begin its mission. Many highly-skilled hackers work diligently to discover new system vulnerabilities that allow the creation of newer ZDEs. These hackers are motivated because ZDEs can be sold for large amounts to bidders such as nation states, or extremists. The ZDEs that are discovered and designed by highly-skilled hackers are a major ingredient for the current generation of cyber weapons.

A final characteristic that enables malicious code to be successful as a cyber weapon is what has been described as an "intimate knowledge" of the targeted industrial control systems of civilian and/or military equipment. The hackers who created the ZDEs that were used in the cyber weapons campaign to attack Iran apparently had a very good understanding of the specific industrial equipment that was targeted. This highly-specialized knowledge held by a designer, and then used to create the various malicious code payloads for espionage and sabotage, is what makes a current generation cyber weapon campaign so effective.

However, there can also be problems with the current generation cyber weapon campaigns. Cyber weapons can possibly go out of control. For example, Stuxnet was reportedly updated several times to add functionality, and eventually the malicious code escaped the confines of the Iranian Uranium Enrichment facility. Instances of Stuxnet have been detected in many countries outside of Iran. However, other facilities have escaped damage because the malicious payload in Stuxnet was designed to attack only the specific equipment inside the nuclear facility in Iran. Future cyber weapons that might not be as carefully designed as Stuxnet could also spread unexpectedly, and might possibly cause collateral damage to other facilities.

In the future, the environment and opportunities for cyberattacks will expand. Past targets have been industrial control systems for critical infrastructures such as oil and gas pipelines, and civilian electrical power stations. As more detailed information for intimate knowledge becomes reachable over the internet, future targets will likely include complex military facilities and weapon systems, including more examples of nuclear facilities, or communication, command and control (C3)/C3 plus computer (C4) systems, and missile defense architectures (like Surface-Air-Missiles). For example, the Soviet-era BUK Missile System Anti-aircraft missile (SAM) system that reportedly brought down Malaysia Airlines Flight 17, killing 298 people over Ukraine on July 2014, is sophisticated, but may have vulnerabilities, and does not possess the ability to discern civilian from military targets on its own. Unfortunately, detailed knowledge of the BUK Missile System is available over the Internet. Technical instructions for this system, plus several Russian-made missile launchers, in the form of an accurate software simulator, can be downloaded from the Internet, enabling anyone to learn and practice the basic operation of multiple Soviet-era antiaircraft missile launchers.

As another example of growing vulnerabilities for sophisticated military equipment, the Defense Science Board reportedly has given the Pentagon a classified list of military weapons systems where designs were stolen by cyber espionage. The list includes designs for the advanced Patriot missile system, known as PAC-3 (see Washington Post, Ellen Nakashima, May 27, 2013). A separate report also available on the Internet shows research on vulnerability analysis of national missile defense software, including the PAC-3 Patriot Missile System ("Using Genetic Algorithms to Aid in a Vulnerability Analysis of National Missile Defense Simulation Software" — JDMS, Volume 1, Issue 4, October 2004 Page 215–223, http://www.scs.org/pubs/jdms/vol1num4/imsand.pdf).

In conclusion, cyberattacks are becoming more sophisticated, and when the following characteristics are present — (a) use of ZDEs to bypass cybersecurity technology, (b) use of campaigns involving coordination of several different malicious programs, and (c) use of stealth to prolong malicious operations for espionage or sabotage — we may be experiencing the effects of a cyber weapon. Correct attribution is very difficult, and the technologies used for cybersecurity defenses are becoming less adequate for the expanding job of protection against cyber weapons. Therefore, classical deterrence theory developed for the nuclear weapons could not work for the cyber weapons. In addition,

cyber weapons can possibly go out of control. Future cyber weapons that are not built as carefully as Stuxnet could also spread unexpectedly and cause unpredictable damage. Finally, research into examples of current generation cyber weapons has also shown that detailed and intimate knowledge of a targeted system contributes to the success of a cyber sabotage campaign. As more information becomes available on the internet describing intimate details and the possible vulnerabilities of sophisticated equipment and facilities, including military equipment, perhaps through cyber espionage, these may also become new targets for future generations of cyber weapons.

There are many policy topics related to cybersecurity and cyber warfare that are worthy of future research:

- Which strategies may help reduce/regulate global proliferation of ZDEs/malware/payloads designed for cyber warfare?
- Future attack campaigns are likely already in place and operating now. How can these be detected and restrained?
- What is, if any, the legality in the framework of international (and humanitarian) law concerning the use/threatened use of nuclear weapons as retaliation against cyber weapons?
- Is a cyber arms control mechanism feasible? If it is, keeping in account that a nuclear arms control system took decades, how long will this take?
- Is the UNSC still the right Institution to deal with a global cyber arms control?
- If yes, to avoid a Cybergeddon, should the P5 reveal all cyber weapons openly?

Санджай Гоел
Университет Олбани, SUNY, США

Исполнимо ли международное законодательство и договоры в киберпространстве: Можем ли мы преодолеть проблему атрибуции посредством технологий?

Добрый день! Я уже девятый год принимаю участие в этом мероприятии, и мне всегда приятно находиться здесь и видеть множество знакомых лиц. Я хотел бы выразить свою самую искреннюю благодарность генералу Шерстюку и ИПИБ за приглашение. Наш мир полон нестабильности, но мы, тем не менее, находимся здесь и объединяем усилия в попытках решить кажущуюся неразрешимой проблему киберконфликтов. Я говорю «кажущуюся» потому что, обращаясь к этим вопросам, мы делаем первый, самый трудный и важный шаг на пути к их решению. Настоящий доклад посвящен процессу и возможности адаптации международного права к киберинцидентам на основе технических и стратегических факторов.

Было предпринято несколько попыток создать международные договоры для противодействия киберпреступности и регламентации киберконфликтов, но достигнуть консенсуса оказалось затруднительным. Каждое государство имеет свою собственную правовую систему с различными законами, в основе которых лежат социальные ценности, политический истеблишмент и социальные нормы, складывавшиеся веками. Международное право создавалось по крупицам, и законы, как правило, принимались после ужасных инцидентов, которые выводили на передний план глобальное самосознание. Мы не видели ничего подобного по своим масштабам в киберпространстве, и в этом заключается одна из причин бездействия.

Политические лидеры уклоняются от изменения политики и законов для решения проблем, которые возникают в свете новых реалий глобализации. Отчасти это происходит, потому что эффективное решение этих проблем влечет за собой необходимость гармонизации законов во всех странах, возможно, что за счет сограждан. Вместо стремления к достижению подлинного компромисса некоторые страны по-прежнему демонстрируют

непримиримую позицию, и при этом лоббируют свои собственные взгляды в других государствах. Это можно рассматривать как уловку, используемую для дальнейшего наращивания арсенала и замедления продвижения других на этом направлении.

Физическое против киберпространства

Некоторые ученые утверждают, что киберпространство не отличается от физического и что существующее международное законодательство должно применяться в обоих случаях. Существует много аналогий при сравнении киберконфликтов с другими формами ведения войны, принципы конфликта могут применяться к обеим формам, и, следовательно, правила ведения обычной войны также применимы и в киберпространстве. Тем не менее, существует достаточно много отличий и особенностей киберпространства, которые в ряде случаев делают невозможным исполнение обычных правил ведения войны. Я считаю, что мы должны изучить существующее международное законодательство, принять его в качестве ориентира — но тщательно проработать уникальные проблемы киберпространства по мере формирования новой международной киберюриспруденции.

Есть несколько отраслей права, которые применимы к киберконфликтам, в том числе:

1. Право вооруженных конфликтов;
2. Право нейтралитета;
3. Гуманитарное право.

Мы рассмотрим каждую из этих отраслей права, связанных с международными конфликтами, и поднимем ключевые вопросы, касающиеся их адаптации к киберпространству с точки зрения существующих проблем атрибуции.

Право вооруженных конфликтов

Право вооруженных конфликтов развивалось через серию соглашений, и имеет несколько положений:

1) *Война должна осуществляться законной властью, проистекающей из принципа государственного суверенитета.*

Что является законной властью в ходе кибервойны? Кибервойна ведётся скрытно, как правило, через прокси-государства. Являются ли прокси-государства легитимными посредниками других государств? Согласятся ли когда-нибудь государства, что субъекты, совершившие нападения, являются их посредниками? Что если прокси действуют за пределами страны?

2) *Война не должна преследовать узкие национальные интересы, напротив, её целью должно быть восстановление справедливого мира.*

Что является справедливым миром в киберпространстве? Может ли быть оправдан упреждающий удар, осуществленный в национальных интересах?

3) *Необходимо оценивать издержки и выгоды участия в войне (в том числе человеческие жизни и экономические ресурсы).*

В ходе кибервойны важна безотлагательность при проведении контратаки. В подобных сценариях зачастую очень сложно дать точную оценку положительных и отрицательных факторов перед осуществлением контратаки.

4) *Необходимо обеспечить пропорциональность ответного удара*

Концепция пропорциональности основана на оценке ущерба, а для проведения такой оценки в случае с киберпространством часто требуется много времени. В связи с необходимостью мгновенной реакции во многих случаях трудно обеспечить пропорциональность.

5) *До применения силы необходимо использовать все дипломатические средства*

Неоднозначность атрибуции и сопутствующие дипломатические разбирательства могут занимать много времени, в то время как потребность в ответных действиях по отражению атаки (и возможном нанесении при этом побочного ущерба) носит безотлагательный характер.

Право нейтралитета (Гаагская конвенция 1907 года)

Право нейтралитета регулирует вопросы сосуществования государств в военное и мирное время. Это право гласит, что нейтральные страны не должны позволять использовать свои ресурсы одним государствам для нападения на другие государства. Это налагает на нейтральные страны следующие обязательства:

- Воздерживаться от участия в конфликте;
- Сохранять беспристрастное отношение к комбатантам;
- Недопущение нарушения нейтралитета воюющими сторонами на их территории;
- В том числе, при необходимости, путем применения силы;
- Интернирование комбатантов, обнаруженных на территории нейтрального государства, до окончания военных действий.

Что означает участие в конфликте в киберпространстве? Нарушает ли принципы права нейтралитета бот-сервер, расположенный на нейтральной территории?

Основная проблема применимости этих законов заключается в слабости национальной киберинфраструктуры. Компьютеры, находящиеся на территории нейтрального государства, могут быть без его ведения взломаны для проведения атаки. Можем ли мы возложить на эти страны ответственность за нападения на другие государства, особенно если нейтральная страна не имеет технических возможностей или ресурсов для адекватного обеспечения безопасности своих сетей?

Эти законы также запрещают противоборствующим сторонам использовать нейтральные территории для перемещения оружия, войск, и т.д., или вербовать комбатантов в нейтральных государствах.

Может ли гражданин нейтральной страны, добровольно работающий с противоборствующей страной, подвергнуть нейтральную страну правовой опасности?

Например, в случае нападения на корпорацию SONY, несколько стран были ответственны и не возникло четкой атрибуции.

Гуманитарное право

Применимости международного гуманитарного права (МГП) к конфликтам в киберпространстве уделяется особое внимание. МГП определяет набор правил, ограничивающих последствия вооруженного конфликта, посредством защиты людей, которые являются некомбатантами или больше не принимают участия в военных действиях, и ограничения средств и методов ведения войны. Несмотря на то, что с некоторыми принципами этого права можно согласиться, необходимо учитывать различия между физическим и киберпространством. В ряде случаев граждане государства сами принимают участие в атаках — являются ли они легитимными целями для контратаки?

Важно также отметить, что интерпретация законов зависит от обстоятельств и точки зрения толкователя. Они могут быть применены неправильно, использованы в узких интересах, или отвергнуты по надуманным основаниям. Законы должны составляться таким образом, чтобы быть однозначными и поддающимися исполнению — что трудно сделать в случае с киберпространством. Для того чтобы скрыть свою личность, нападающие могут использовать анонимность, обеспечиваемую Интернетом. В этом заключается трудность в обеспечения соблюдения правил. Есть несколько явных факторов, которые усложняют решение проблемы исполнимости законов и неоднозначности — особенно в вопросах противодействия киберпреступности.

Мотив

Так как спецслужбы и вооруженные силы государств все чаще занимаются шпионажем и подрывной деятельностью против других стран в киберпространстве, различия между киберпреступностью и кибервойной размываются. Политическому руководству государства трудно определить, являются ли нападения на вебсайты или похищение данных через Интернет делом рук отдельных лиц в другом государстве (движимых личной выгодой, политическими или религиозными убеждениями), или действиями разведки или вооруженных сил этого государства. Поскольку мотивы остаются неясными, становится очень трудно отличить потенциальные акты кибервойны от киберпреступности.

Атрибуция

Атрибуция является одной из главных проблем при исполнении права ведения кибервойны. Должны ли мы быть в состоянии однозначно идентифицировать лиц, совершивших преступления, чтобы применить нормы международного права? Есть три категории проблем атрибуции. Во-первых, как известно, трудно осуществить атрибуцию атак через Интернет. Злоумышленники могут маскировать свои действия, пользуясь недостаточной защищенностью многих хост-серверов, что позволяет им использовать машины в третьей стране для атак. Без надлежащего трансграничного сотрудничества или наблюдения трудно получить высокий уровень уверенности в атрибуции. Вторая проблема касается атак на защищенные системы посредством других средств хранения информации, таких как флэш-накопители, компакт-диски и DVD-диски. Примером такой атаки является вирус Stuxnet, внедренный в системы иранских ядерных объектов. В случае таких защищенных систем происхождение оружия должна определить экспертиза и разведка. Третья проблема атрибуции заключается в предустановленных в программно-аппаратную часть вредоносных функциях.

Техническая атрибуция

Для проведения технической атрибуции требуется соответствующий анализ сетевого трафика — сбор данных из различных источников, и затем построение цепи доказательств с целью определения виновных. Если мы можем вовремя собрать доказательства, то есть методы проведения надежной атрибуции, однако ключевой проблемой в процессе сбора данных является

их распределенность по сети. В наличии может быть несколько фрагментов информации, но они могут быть подделаны для затруднения атрибуции.

Атрибуция по IP-адресу является менее полезной, если IP-адрес хоста, который инициировал нападение, был фальсифицирован, или принадлежит промежуточному хосту. Или может оказаться так, что IP-адрес был присвоен во время того действия, атрибуцию которого мы проводим.

В случае с атаками, проведенными с помощью электронной почты, знание адреса электронной почты потенциально является важным способом выявления источника — хозяина электронной почты, и, в конечном счете, преступника. К сожалению, по причине того, что адрес электронной почты легко создать или подделать, он зачастую является тупиковым путем для атрибуции.

Выявление физического местоположения источника атаки важно для установления юрисдикции и получения ордера на обыск или принятия других соответствующих мер в случае совершения преступления, акта терроризма или войны.

Идентификация конкретного человека, который работал за атакующим компьютером является последним шагом атрибуции. Тем не менее, кроме установления личности, для полноты атрибуции может также потребоваться определить, действовало ли данное лицо от имени иностранного правительства, террористической организации или преступной группы.

Рассмотрим эпизод с взломом систем корпорации SONY

- Анализ вредоносных программ, использованных при нападении, показывает сходство с ранее обнаруженными вредоносными программами, происходящими из Северной Кореи. Сходство было в программном коде, алгоритмах шифрования, методах удаления данных и взломанных сетях.
- Было также отмечено, что некоторые IP-адреса, связанные с группой северокорейских предприятий, расположенных в Шэньяне на северо-востоке Китая, были жестко закодированы в использованные вредоносные программы удаления данных.
- Примененные в этой атаке инструменты также имели сходство с инструментами, использованными в кибератаке на южнокорейские банки, предположительно осуществленной КНДР в марте 2015 года.

Как можно видеть, больш*ая* часть атрибуции является гипотезой, основанной на косвенных доказательствах. Она также в значительной степени опирается на IP-адреса, которые, как мы все

знаем, могут быть подделаны, иногда намеренно, для дезинформации. Кроме этого, доказательства строятся на основе данных частных поставщиков, а источники этих данных по-прежнему остаются тайной. Если мы не изменим стандарты атрибуции, она будет оставаться слабой и не будет иметь правовой силы в суде. В этом и заключается трудность противодействия кибератакам.

Какое есть будущее у атрибуции?

Невероятно трудно установить множество фактов о любой атаке, поскольку осуществление кибератак одного государства на другое может быть передано частным подрядчикам и осуществляться посредством бот-сетей, состоящих из компьютеров-зомби ничего не знающих людей и организаций, распределенных по всему миру. Эти факторы значительно усложняют сбор достаточного объёма доказательств для определения, кто на самом деле несет ответственность, и/или мотива нападения. Однако, установление ответственной стороны (сторон) и мотива является решающим фактором для определения того, должно ли преступление быть предметом судебного разбирательства в рамках права вооруженных конфликтов. Когда военнослужащие осуществляют атаку в физическом пространстве с помощью таких обычных вооружений как огнестрельное оружие, пушки, самолеты и ракеты, то факты, говорящие о том, кто стрелял в кого, вначале могут быть запутанными и скрытыми намеренной дезинформацией. Тем не менее, есть отчеты независимых журналистов и очевидцев, быстро растущее количество материалов спутниковой аэрофотосъемки и разведки, а также фотографии и видеозаписи, сделанные гражданскими лицами и военнослужащими, и быстро загруженные в Интернет. В киберпространстве сложно определить, что нападение уже осуществлено, не говоря уже о том, где и кем. Более того, учитывая, насколько трудно провести атрибуцию ответственности за кибератаки, жертве нападения трудно реагировать должным образом (т.е. пропорционально) в соответствии с правом вооруженных конфликтов.

Если атакованное государство не может эффективно реагировать точно направленной контратакой, то государства не могут убедительно угрожать наказанием странам, инициирующим кибератаки. Не имея такой убедительной угрозы, государства не в состоянии эффективно сдерживать другие государства от проведения кибератак — подобно тому, как они способны сдерживать атаки в физическом пространстве обычным или ядерным оружи-

ем. Отсутствие возможности убедительно угрожать атакующим государствам ответным наказанием серьёзно подрывает эффективность применения мер коллективной безопасности группами государств или международным сообществом. Даже если государства мира договорятся, подпишут и ратифицируют универсальный мирный договор для киберпространства, то, учитывая сложность его исполнения, отдельные государства смогут легко нарушать этот договор, не опасаясь возмездия.

Что делать? Возвращаясь к вступительному слову, вопросы международной киберпреступности и кибервойны, «кажутся» неразрешимыми. Сейчас я уделил много времени подробному рассмотрению текущих вопросов, дилемм и трудностей, связанных с атрибуцией и ответными действиями на киберпреступность, и которые, как кажется, резко ограничивают применимость норм международного права в киберпространстве. Тем не менее, нормы и заложенные в них принципы — международное сотрудничество, ответственное отношение к законности и взаимовыгодная безопасность для всех — это ориентиры, которые должны направлять нас в работе по созданию технических средств для улучшения возможностей атрибуции и судебной экспертизы. Для установления происхождения кода, а затем и атрибуции, во все большей степени используется анализ вредоносных программ. Со временем атрибуция станет более надежной, и к этому моменту нам нужно подготовить правовые документы и политический консенсус, чтобы совместно, как международному сообществу, эффективно решать кибервопросы.

Подобно тому, как мир после Второй мировой войны обратился к международному праву для регулирования и обеспечения безопасности в новой реальности, созданной ядерным оружием, мы должны быть непоколебимы в наших усилиях по достижению международного консенсуса по вопросам регулирования киберпреступности и кибервойн. Существующие в настоящее время технические проблемы атрибуции постоянно изменяются; однако необходимость в сотрудничестве и эффективной юриспруденции, всегда актуальна, универсальна и гораздо важнее, чем технические препятствия, которые мы должны преодолеть.

Интернет быстро превращается из общественного собрания и рынка в зону конфликта, где угроза исходит от многих акторов. Мы находимся на грани; мы можем сохранить Интернет, как ресурс для нашего и будущих поколений во всем мире — независимо от страны происхождения, политических или религиозных убеждений; или позволить ему быть уничтоженным взаимным

недоверием и ограниченными интересами. Будучи оптимистом, я верю, что нам удастся сохранить его полезность. Я твердо верю, что трудности, которые были подробно рассмотрены сегодня, преодолимы, если мы будем уверенно идти к построению консенсуса. Мы должны выработать общие цели, объединяя экспертизу, разведку, право и политику, совокупность которых может лечь в основу международного киберфорума.

Нам предстоит многое сделать для понимания проблем и поиска решений, которые будут справедливы для всего сообщества, в том числе найти баланс конкурирующих интересов государств. Форум в Гармише будет продолжать играть важную роль в этом начинании.

Спасибо большое за ваше время и внимание.

Sanjay Goel
University at Albany, SUNY, USA

Are international laws and treaties enforceable in cyberspace: Can we overcome the attribution challenge through technology?

Good Afternoon! This is my 9th year at this event, and it is always a pleasure to attend, and see so many familiar faces. I would like to offer my sincerest thanks to General Sherstyuk and IISI for inviting me. Ours is a world full of turmoil, yet we stand here united in our effort to solve the seemingly intractable problem of cyber conflicts. I say 'seemingly' because, by facing these issues we are taking the first, most difficult and important step towards resolution. This talk is focused on the adaptation, and adaptability of international law to cyber incidents based on both technical and strategic considerations.

There have been several efforts to draw international treaties to address cyber crime and regulate cyber conflict, yet reaching consensus has been difficult. Each state has its own legal system with diverse laws based on societal values, political establishment, and social norms developed through centuries. International law has been painstakingly developed, with laws typically enacted following horrific incidents that brought global consciousness to the fore. We have not seen anything of similar proportion in cyberspace, and therein lies one reason for the inertia.

Political leaders are reluctant to face the new realities of globalization by changing policies and laws to address the problems that come with it. Partially, the reluctance is because effectively addressing these problems entails harmonizing laws across all countries at the potential expense of the domestic audience. Instead of striving for genuine compromise, some countries continue to reiterate intransigent positions while lobbying their own views on other countries. This can be seen as using subterfuge to continue building an arsenal while working to slow others down in the same pursuit.

Physical vs Cyber

Several scholars have argued that the cyber domain is not distinct from the physical, and that current international laws should apply to both. There are a lot of analogies between cyber conflict and other

forms of warfare, the principles of conflict can apply to both, and consequently, the rules of conventional warfare also apply to cyberspace. However, there are enough differences and singularities in the cyber domain to make the enforcement of conventional rules of warfare untenable in several cases. I believe we need to learn from existing international laws — to take them as a guide — but seriously think through the unique issues of the cyber domain as we build new international cyber jurisprudence.

There are several laws that are applicable to Cyber Conflict, including:

1. Right to Armed Conflict
2. The Law of Neutrality
3. Humanitarian Law

We examine each of these laws dealing with international conflicts and raise key issues regarding their adaptation to the cyber domain given issues of attribution.

Right to Armed Conflict

The right to armed conflict has evolved through a series of agreements, and has several clauses:

1) *War should be waged by a legitimate authority rooted in the notion of state sovereignty.*

In cyber conflict, what is a legitimate authority? Cyber warfare is a covert warfare typically conducted by proxies of countries; Are the proxies of nation states legitimate? Would nation states ever agree to the notion that the entities committing the attacks are their proxies? What if the proxies are operating outside of the country?

2) *The aim of war must not be to pursue narrowly defined national interests, but rather to re-establish a just peace.*

What is just peace in cyber space? Can a pre-emptive strike for national interests be justified?

3) *The need to weigh the costs and benefits involved in waging war (including human life and economic resources).*

There is a need for immediacy in cyber warfare while launching a counter attack. It is often difficult to make an accurate assessment of the pros and cons of such an attack in such scenarios.

4) *The need to ensure that counter attack be proportional to the violence being encountered.*

The concept of proportionality is based on an assessment of damage, which often takes a long time to analyze in the cyber world. This need for immediacy of reaction makes it difficult to ensure proportionality.

5) *We must exhaust diplomatic options prior to violence.*

Ambiguity in attribution, and resultant diplomatic wrangling can be long processes, while the need for response to repulse the attack (and cause collateral damage) has great urgency.

The Law of neutrality (Hague Convention V of 1907)

The Law of neutrality regulates the coexistence of states at war and states at peace. This law asserts that neutral countries should not allow their resources to be used by one country to attack another. It places the following responsibilities on neutral countries:

- Refrain from participating in the conflict
- Maintain impartial treatment of combatants
- Prevent belligerents from committing violations of neutrality on their territory
- Including use of force if necessary
- Intern combatants found on territory until end of hostilities

What does participation mean in the cyber domain? Does a bot server located on neutral territory violate the tenets of the Law of neutrality?

The fundamental problem with the applicability of these laws is the weakness of national cyber infrastructure. Computers of a neutral country can be infiltrated without its cognizance in order to launch an attack. Can we hold these countries responsible for the attacks launched by other countries, especially if the neutral country does not have the technical ability or resources to adequately secure their networks?

These laws also prevent combating parties from using neutral territories to move weapons, troops, etc., or recruiting combatants from neutral states.

Can the citizen of a neutral country working voluntarily with a combating country put the neutral country in legal jeopardy?

In the case of the attack on SONY, for example, multiple countries were responsible and the attribution was never clear.

Humanitarian Law

There has been a particular emphasis on the application of the International Humanitarian Law (IHL) to cyber conflict. IHL defines a set of rules that limit the effects of armed conflict (LOAC) by protecting individuals who are not, or are no longer, participating in the hostilities, and it restricts the means and methods of warfare. While one

may agree with the principles underlying this law, unique differences between the cyber and physical domains must be considered. In several instances the citizens of a country are involved in launching attacks themselves — are they legitimate targets of a counter attack.

It is important to note that laws are subject to interpretation based on circumstances and point of view. They can be applied erroneously, inconsistently, misused for parochial reasons, or flouted for reciprocity, based on flimsy grounds. The laws need to be defined so that they are unambiguous and enforceable, which is difficult in the cyber domain. Attackers can use the Internet's cloak of anonymity to camouflage their true identities. There are several explicit factors that make enforceability and ambiguity issues particularly difficult for cyber crimes.

Motive

As intelligence agencies and militaries of states are increasingly engaging in espionage and subversive activities against other nations in cyber space, distinctions between cyber crime and cyber warfare are blurring. It is difficult for the leadership of one state to distinguish whether attacks on a website or online theft of data are actions of individuals in another state who are motived by financial gain, political or religious ideology, or actions taken by that state's intelligence agency or military. Since motive is unclear, it becomes very difficult to differentiate potential acts of cyber war from cyber crime.

Attribution

Attribution is one of the largest challenges in the enforcement of cyber warfare rules. Must we be able to unambiguously identify the perpetrators of a crime to apply an international law? There are three categories of attribution problems. First, attacks through the Internet are notoriously difficult to attribute. Attackers can camouflage their actions by exploiting a lack of security on many hosts, allowing them to use machines in a third country for launching attacks. Without proper cooperation or surveillance across borders, it is hard to have high confidence in attribution. The second problem deals with delivering attacks on secure systems through other media, such as thumb drives, CDs and DVDs. An example of this was the Stuxnet worm introduced into Iranian nuclear facilities. For these secure systems, forensics and intelligence should identify the source of the weapon. The third attribution issue is malware in the hardware and software that is preloaded.

Technical Attribution

Technical attribution requires network forensics, such that data is collected from various sources, and then a chain of evidence is built to identify the perpetrators. If we are able to collect evidence in time we have techniques to provide reliable attribution, however the key challenge in data collection is its dispersion across the network. There are several pieces of information that are available but information can be spoofed making attribution harder.

IP address attribution is less useful if the IP address of the host that initiated the attack is spoofed, or belongs to an intermediate host. One may also be able to discover the machine assigned the IP address at the time of the attributed action.

For attacks conducted via e-mail, knowing the e-mail address potentially serves as a useful way to identify the source computer, e-mail address holder, and ultimately the perpetrator. Unfortunately, since e-mail addresses are also easy to create or spoof, an e-mail address is often a dead end for attribution.

Locating the physical location of the source of the attack is important so that jurisdiction can be established, and search warrants or other actions can be taken, as appropriate in the case of crime, terrorism, or war-like activities.

Identifying the actual individual who was at the attacking computer is the final step of attribution. However, beyond identifying the individual, sufficient attribution may also require determining whether the individual was acting on behalf of a foreign government, terrorist organization, or criminal group.

Consider the SONY hack

- analysis of the malware use in the attack shows similarity to previous malware linked to North Korea. The similarities were in lines of code, encryption algorithms, data deletion methods, and compromised networks.
- It was also noticed that several Internet protocol (IP) addresses associated with a group of North Korean businesses located in Shenyang in northeastern China were hardcoded into the data deletion malware used in this attack.

The tools used in this attack also had similarity to a cyber-attack against South Korean banks carried out purportedly by North Korea in March 2015.

As you can see here, a lot of the attribution is conjecture, based on circumstantial evidence. It also largely rests on ip-addresses that we

all know can be spoofed, sometimes deliberately, to misdirect attacks. Also, the evidence is based on private-vendor data and the sources of the data are still secret. Unless we change the standards of attribution, this seems like weak attribution that would not stand in any court of law. Therein lies the difficulty in responding the cyber attacks.

What is the future of attribution?

The fact that cyber attacks by one state on another can be outsourced to private contractors, conducted through botnets of the zombie computers of unknowing people and organizations, and distributed across the globe, makes it incredibly difficult to ascertain many facts about any given attack. These factors greatly complicate the gathering of sufficient evidence to establish who is actually responsible, and/or a motive behind an attack. Yet, the responsible party (ies), and a motive, are critical factors to ascertain if the crime is to be subject to adjudication informed by the Law of Armed Conflict. When military personnel conduct an attack in physical space using conventional weapons, like guns, cannon, aircraft and rockets, the facts of who shot whom first may be complicated and shrouded in self-serving disinformation. Nevertheless, there are reports of independent journalists and eyewitnesses, a rapidly growing body of satellite imagery and aerial reconnaissance, as well as photos and videos taken by civilians and military service personnel that are often quickly uploaded to the Internet. In cyberspace, ascertaining that an attack even occurred, let alone from where and by whom is fraught with difficulty. Moreover, given that it is so difficult to attribute responsibility for a cyber attack, it is difficult for the victim of the attack to respond in a manner (ie proportionately) as justified by the Law of Armed Conflict.

If a state that has been attacked cannot effectively respond with an accurately aimed counterattack, states cannot credibly threaten to punish any state that initiates a cyber attack. Lacking such credible threats, states are unable to effectively deter other states from launching cyber attacks as they may be able to deter attacks conducted in physical space, whether by conventional or nuclear weapons. Without the ability to credibly threaten attacking states with retaliatory punishment, any effective enforcement of collective security arrangements among groups of states or the international community is seriously undermined. Even if the world's states were to negotiate, sign and ratify a universal cyber peace treaty, individual states could easily violate the treaty without fear of retribution, given the difficulty of enforcement.

What to do? I take you back to my opening statement, that these issues of international cyber crime and conflict are 'seemingly' intractable. I have just spent considerable time detailing current issues,

dilemmas and difficulties associated with attribution and retribution in cyber crime, which seem to dramatically limit the applicability of established international law in the cyber domain. However, these laws, and the principles behind them—international cooperation, responsibility for justice, and mutually beneficial security for all—are precisely the beacons that must guide us as we work to establish the technical means to improve attribution and forensics capabilities. Increasingly. the analysis of malware is being used to establish provenance of the code and subsequently to establish attribution. Over time, attribution will become more reliable and we need to be ready with the legal instruments and political consensus to effectively deal with cyber issues as an international community.

Just as the world turned to international law after World War II for regulation and security in the new reality of nuclear weapons, we must be steadfast in our efforts to build a foundational international consensus to regulate cyber crime and cyber warfare. The technical issues of attribution that currently exist are evolving as we speak; the need for cooperation, and effective jurisprudence, however, are timeless, universal, and much more important than the technical hurdles we must overcome.

The Internet is quickly transforming from a community gathering and marketplace to a conflict zone with threats from multiple actors. We stand at a threshold; we can preserve the Internet as a resource for ours and future generations around the world, regardless of country of origin, political or religious affiliation; or allow it to be destroyed through mutual distrust and parochial needs. As an optimist, I trust that we will be able to prevail and maintain its goodness. I strongly believe that the difficulties we've detailed here today are surmountable; by a steadfast dedication to consensus-building. We need to establish mutual goals in a combination of forensics, intelligence, law and politics that can form the basis of an international cyber forum.

We have a lot of work to do in understanding the problems and finding solutions that are fair to the entire community, including balancing competing interests of nation states. The Garmisch Forum has and will play an important role in this endeavor.

Thank you very much for your time, and kind attention.

П.Л.Пилюгин, А.А.Сальников

Институт проблем информационной безопасности
МГУ имени М.В.Ломоносова

Перспективы применения международных правовых норм в киберпространстве

Применимость международного права в киберпространстве

При исследовании и анализе применения правовых норм для обеспечения информационной безопасности и правового регулирования киберпространства чаще всего обращают внимание на распространение в киберпространство фундаментальных принципов (гуманитарных, нераспространения, собственности, свободы слова, защиты личности и т.д.) и принципов международного права, закрепленных в уставе ООН [1–3].

Другой поиск подходов к правовому регулированию в киберпространстве строится на методах аналогии с регулированием космического пространства, воздушного пространства, территорий Антарктиды и т.д. [4]

И такие аналогии не всегда корректны. Основная причина в том, что хотя перечисленные выше объекты и вовлечены в деятельность человечества (иначе бы таких норм не было), степень их использования по сравнению с общими объемами человеческой деятельности относительно не велика. А киберпространство, напротив, затрагивает уже почти все сферы деятельности. Такой подход мог быть справедлив в отношении киберпространства лет 20–30 назад, с последующим развитием «кибер права» и делением его на различные разделы и направления по мере развития использования киберпространства. В настоящее же время проблема настолько усложнилась, что рассматривать это пространство как целое разумно только с философской точки зрения, а практика требует существенно большей детализации.

То, что мы сейчас называем киберпространством, по сути является надстройкой над развитой инфраструктурой передачи данных, над сетью Интернет. Поэтому наиболее популярными являются подходы, которые предполагают представление основы киберпространства — сети Интернет, как системы связи или транспортной системы [4, 5].

В общем, сеть Интернет — это, безусловно, система связи, как по назначению, так и по социальным последствиям, напри-

мер, которые оказали системы связи на общество (прежде всего, радио и телевидение). Однако сеть Интернет, это не просто сеть связи, а вычислительная сеть, сеть пакетной передачи данных, она существенно более сложна, но и более гибка и универсальна. По сути, это дальнейшее развитие систем связи, которое требует и развития соответствующих норм, и регламентирующих документов, а стремительное развитие именно сети пакетной передачи данных — сети Интернет привело к тому, что правила предшествующих систем связи не переносимы в сетевую структуру.

Вместе с тем, если вспомнить, что Интернет создавался, именно как транспортная среда, как сеть передачи пакетов информации (IP пакетов данных) — информационного трафика, и вся эта деятельность уже является отдельной отраслью, то можно заметить, что сложившаяся экономическая практика вполне соответствует деятельности операторов неинформационных транспортных систем (пароходных, авиационных, железнодорожных и прочих транспортных компаний). В соответствии с этой аналогией можно попытаться использовать принципы правового регулирования, обеспечения безопасности, полученные в течение многолетней практики неинформационных транспортных систем, в информационной траспортной инфраструктуре и использовать методологию, подходы и практику сложного и многообразного транспортного права [5] и правил регулирования транспорта [6–8] для поиска правовых решений, связанных с более детальным представлением сети Интернет и киберпространства, которое она обеспечивает.

Многоуровневая модель глобальной сети

При анализе деятельности глобальной сети Интернет для упрощения рассматриваемых задач используют многоуровневую модель ISO/OSI или более простую модель TCP/IP, которая лежит в основе сети Интернет. Рассмотрим эти уровни, используя предложенный выше подход сравнения сети Интернет с различными транспортными системами.

Канальный уровень — это реальные объекты: волоконная оптика, спутники связи, витая пара, устройства сопряжения, простейшие коммутаторы и т.д. и правила их взаимодействия.

В соответствии с предложенной аналогией, можно привести в качестве примера автомобильные или железные дороги с устройствами их обеспечения (стрелки, подстанции и т.д.). Сюда же можно отнести (с учетом их специфики) морские и речные пути, воздушное пространство для авиасообщений или коммуникации

для перекачки газа и нефти. Все это физические материальные объекты (или среды), попадающие под национальное и международное законодательство и правила регулирования. Такими регулирующими организациями для физических линий связи являются, в частности, Международный союз электросвязи и др.

Сетевой уровень — это уровень организации взаимодействия по совокупности этих линий связи и он также обладает физическими устройствами, для удобства совмещенными с оборудованием физического (и следующего транспортного) уровня — прежде всего это маршрутизаторы и коммутаторы.

По аналогии с предыдущим уровнем, здесь можно рассматривать, как транспортные средства, так и средства управления движением. Для железных дорог — это локомотивы, вагоны, системы управления движением и пр. Легко привести аналогии и для других видов транспорта. Все это не только логические и организационные структуры, но и физические материальные объекты, и как материальные объекты они должны попадать под национальное и международное законодательство и специальные правила регулирования. Сегодня такими специализированными регулирующими организациями являются, в частности, ICANN, IANA и др.

Транспортный уровень — это уровень более сложных протоколов, обеспечивающих через сеть информационный обмен между отдельными хостами, устройствами, программами, серверами и персональными компьютерами (точнее их компонентами, отвечающими за информационный обмен).

В качестве аналогии приведем примеры: логистику, организацию грузооборота и пассажиропотока между станциями, вокзалами, портами, аэродромами и т.д. Все это также не только организационные структуры, но и физические материальные объекты, и как материальные объекты они должны попадать и под национальное, и международное законодательство и под правила регулирования. Сегодня такими регулирующими организациями исторически являются ICANN, IANA и др.

Уровень приложений — по сути это и есть киберпространство, где взаимодействуют люди и созданные ими программы (в некотором смысле уже это искусственный интеллект), которым для реализации этого взаимодействия нужны и персональные компьютеры (или другие устройства взаимодействия человека с сетью), и сервера и т.д.

Используя те же аналогии, можно рассматривать товарообмен между организациями, людьми и, собственно, передвижение

людей по транспортным путям. Здесь уже важно не только количество, но и содержание: конкретные виды товаров, миграции населения и т.д. Все это также должно попадать под национальное и международное законодательство. На этом уровне также существуют услуги, повышающие удобство взаимодействия с транспортной системой. Для обычных транспортных систем это транспортные агентства, службы обеспечения питания, подготовки багажа и пр. В сети Интернет это более удобная система именования ресурсов сети — служба доменных имен (DNS) и базы данных инфраструктурной информации (сервис whois), правила регулирования которых исторически вводились и поддерживаются теми же регуляторами (ICANN, RIPE и др.).

Из приведенного выше видно, что вопрос сетевого регулирования киберпространства касается, прежде всего, сетевого и транспортного уровней. Прикладной же представляет интерес в части сервисов (услуг), которые обеспечивают и «управляют» сетевым и транспортным уровнем — например, DNS и БД инфраструктурной информации, в остальных же случаях можно попытаться опираться на уже существующие нормы. Ниже рассматривается задача обеспечения сетевой безопасности на основе предложенного подхода (на сетевом и транспортном уровнях).

Особенности безопасности сети

Когда говорят о безопасности сети, подразумевается обеспечение информационной безопасности, связанное с глобальной сетью, с элементами ее сетевого, транспортного и отчасти прикладного уровней и прежде всего, с элементами критически важных информационных инфраструктур (КВИИ).

Безопасность сетевого и транспортного уровня подразумевает: доступность и целостность при информационном обмене, а также в некоторых случаях защиту трафика информации и информации управления сетью (обеспечение конфиденциальности). С позиций сетевого и транспортного уровней, даже если не рассматривать особенности разных видов сетевых атак, можно отметить, что обеспечение доступности, имитостойкости и конфиденциальности связано не только с уничтожением, перехватом или внедрением вредоносного трафика, но и с проблемами адресации и организации движения трафика: маршрутизации и поддержания системы доменных имен в целом [10].

Идеология построения глобальной сети предполагает, что она представляет собой согласованное объединение отдельных сетей — автономных систем Интернета (взаимодействие между

которыми осуществляется на основе специальных протоколов), что обеспечивает высокую живучесть и надежность сети при неукоснительном соблюдении правил межсетевых взаимодействий. Однако точность и неукоснительность выполнения правил регулирования не всегда осуществляется на должном уровне, а при противоправных действиях (в военных или преступных целях) сознательно нарушается, да и сами протоколы взаимодействия нуждаются в развитии и доработке.

Другой особенностью является то, что атаки на элементы сети осуществляются через саму сеть, через ее сетевой и транспортный уровни [10]. Если использовать приведенные выше аналогии для этих уровней — это атаки на элементы транспортной инфраструктуры: дороги, мосты, станции, порты, суда и т.д. (что уже не раз было в мировой практике). Причем предполагается, что источник атаки априори допускается до этой инфраструктуры и ограничен только регламентами ее использования.

Еще одна важная особенность сетевых атак состоит в том, что их осуществление упрощается, если проводить их с позиций провайдера (т.е. с позиций, когда возможен непосредственный доступ к элементам сети) или других непосредственных участников этой деятельности, а для атак на маршрутизацию или систему доменных имен это существенно важно. Если использовать предыдущую аналогию, то можно сказать, что источник атаки не только допускается до этой инфраструктуры, но и является ее собственником или модератором, т.е. практически не ограничен в возможностях ее использования.

Более того, как уже упоминалось выше, вся деятельность по информационному обмену — это торговля IP-трафиком, и если бы экономического стимула не было, то и сеть перестала бы существовать. Основными выгодоприобретателями здесь являются провайдеры, осуществляющие пиринг и транзит Интернет-трафика, а через них и других пользователей сети свою прибыль имеют производители оборудования. На эти же средства существуют и регуляторы, и отчасти различные контент-провайдеры, такие как Google, Facebook, и др. (однако это уже относятся к прикладному уровню, где существуют еще и свои каналы финансирования). Вполне понятно, что все выгодоприобретатели и прочие, связанные с ними, заинтересованы в обеспечении безопасности и надежности сети (иначе услуга не будет пользоваться спросом). Но это касается только условий, когда эту выгоду можно получить! Действительно, в любом случае нарушения нормальной экономической деятельности из-за внешних

(революция, военное положение, национализация, банкротство и т. д.) или внутренних причин никакая из перечисленных выше организаций не имеет стимула для поддержания надежности и безопасности сети. Единственной заинтересованной стороной остаются только пользователи сети (люди, кампании, государственные учреждения).

Расследование и объективизация фактов сетевых атак

Исследование возможностей предотвращения, противодействия и расследования таких атак через сеть упирается в трудность их выявления и атрибуции.

Во-первых, достаточно сложно определить, была ли это ошибка проектирования и создания программного кода или на самом деле имела место компьютерная атака. Дело в том, что любое программное обеспечение (ПО) содержит ошибки, последствия которых могут быть катастрофическими. Примеров реальных катастроф с большим числом человеческих жертв или с огромными экономическими потерями из-за ошибок ПО достаточно, и причинами были именно ошибки проектирования или создания программного кода, а не кибероружие или программные закладки. Все это требует тщательного изучения программного кода при анализе инцидентов, а при отсутствии исходного кода ПО, предназначенного для чтения человеком, эта задача может быть чрезвычайно сложной и сравнимой по трудоемкости с созданием аналогичного ПО.

Во-вторых, необходимо выявить источник атаки. Во всем известной кибератаке вирусом Stuxnet виновность США и Израиля в создании кода так и не была доказана [11], хотя иногда можно обнаружить источник сетевых DDOS-атак, которые в сети идут постоянно. Как правило, это действия хакерских групп, а не кибервойск государства. А для целенаправленных атак все значительно сложнее. Дело в том, что все существующие системы «обнаружения вторжений» на самом деле обнаруживают только признаки действий, похожих на вторжение или изменения в системе, а анализ зарегистрированных действий, изменений в системе и машинного кода осуществляется специалистами. Более того, когда внедрение было обнаружено значительное время спустя, то никаких регистрационных данных уже не остается и для определения источника необходимо изучить машинный код внедренных программ, а создатели таких программ автографов, как правило, не оставляют.

Как видно из описанных выше проблем, связанных с распознаванием атаки, определить ее причины и источник, обеспечить атрибуцию фактов преступного использования ИКТ только техническими средствами не удастся. Необходимо будет проводить расследования по каждому такому инциденту для определения его истинных причин и, в случае выявления преступных действий, для фиксирования полученных доказательств.

Такие же подходы используются и в существующих транспортных системах. Это справедливо не только в отношении международных комиссий, расследующих крупные авиационные, железнодорожные или морские катастрофы, но и при поиске пропавших грузов, нарушениях движения, взыскании компенсации за убытки по вине перевозчика и т.д. Если причина инцидента неочевидна, то работа таких комиссий, как правило, начинается со сбора и проверки информации о квалификации персонала и качестве транспортных средств, их обслуживании, проверках, сертификации и т.д., так как это позволяет не только выявить возможные причины инцидента, но и создать основу для дальнейшей работы.

В случае проведения таких расследований для корректной атрибуции фактов сетевых атак, кроме мероприятий по организации таких расследований уполномоченными специалистами, необходимо предусмотреть требования к программному обеспечению, которое будет исследоваться:

- программное обеспечение должно быть официально установлено (приобретено);
- программное обеспечение должно быть подписано надежным сертификатом разработчика;
- разработчик должен хранить (или передать) исходные коды установленного ПО для последующего анализа;
- все изменения программного обеспечения (доработки, модификации, исправления ошибок) должны быть подписаны, а их исходный код сохранен.

Подобные требования к ПО можно рассматривать как сертификацию программного обеспечения, которое должно быть в тех узлах информационной инфраструктуры, которые могут быть подвержены атаке и их необходимо защищать. Кстати, в существующих транспортных системах использование несертифицированного оборудования и путей сообщения, построенных с нарушениями регламента, давно запрещено, причем, не важно, кто был производитель (Boeing, Airbus или ТУ).

Другой важный фактор атрибуции фактов сетевых атак — это устранение анонимности. В существующих транспортных системах, когда последствия преступных действий могут быть значительны (авиационный, железнодорожный, морской транспорт), уже давно никто не путешествует инкогнито, а грузоперевозки осуществляются только поименованных заказчиков. Вся информация фиксируется в именных билетах и товарных накладных. Правда анонимность до сих пор сохраняется при перевозках общественным транспортом или при использовании части почтовых отправлений, но вызвано это скорее не желанием сохранить анонимность, а сложностью фиксации информации при массовых перевозках или почтовых отправлениях. Во всяком случае, здесь используются другие средства фиксации информации, а именно системы видеонаблюдения в транспорте, общественных местах и т.п.

Аналогичные подходы можно использовать и для пользователей глобальных сетей. Речь не идет о том, чтобы посылать фото пользователя с каждым отправляемым им IP-пакетом. Но провайдер для получения оплаты заключает договора на обслуживание с физическими и юридическими лицами. Кроме того, многие контент-провайдеры уже используют мобильные устройства пользователей как средства аутентификации или платежные терминалы. То есть, внедрение функции аутентификации любого субъекта, взаимодействующего с глобальной сетью, технически осуществимо, а результаты такой аутентификации должны быть доступны только в случае проведения расследований, что позволит не нарушать право на сохранение коммерческой тайны или тайны частной жизни.

Важнейшим источником информации при проведении расследований являются различные средства регистрации. В обычных транспортных системах, кроме БД управляющей информации, используются «черные» ящики, фиксирующие основные события, происходящие на транспортном средстве.

В случае расследования сетевых атак такая информация часто оказывается недоступной. Это связано прежде всего с тем, что количество событий, происходящих в сети, слишком велико, и системы регистрации не в состоянии хранить такие объемы информации или это становится слишком накладно. Здесь уместно сделать три замечания. Во-первых, системы регистрации используются в разных целях и хранят с позиции обеспечения безопасности избыточную информацию — выделение и хранение наиболее важной информации позволит уменьшить объемы хранимой

информации и увеличить время ее хранения. Во-вторых, наиболее технологически сложными с точки зрения систем регистрации являются магистральные узлы сети, где электронное оборудование уже отстает от скоростей, обеспечиваемых оптоволоконными линиями связи. В этом случае можно рекомендовать распределять функцию регистрации по менее скоростным узлам. И, наконец, в-третьих, переход к протоколу IPv6 позволяет включать в сами «транспортные средства» сети дополнительную информацию, хотя это и повлечет увеличение накладных расходов — но обеспечение безопасности не бывает бесплатным.

Предотвращение сетевых атак

Более эффективно для обеспечения безопасности не просто обнаружить и выявить источники сетевой атаки, но и предотвратить ее, избежав возможных негативных последствий.

В существующих транспортных системах это обеспечивается:

- правилами пользования транспортом;
- регламентами эксплуатации транспортной сети;
- стандартами для транспортных средств и путей;
- введением административной и уголовной ответственности за нарушение этих правил и регламентов.

В информационной сети роль таких правил и регламентов выполняют различные ISO, RFC и правила подключения пользователей к сети. Однако юридической силы ни RFC, ни ISO (если они не продублированы национальным стандартом — для РФ это ГОСТ) не имеют. Т.е. являются стандартами и правилами «де-факто», которых, по сложившейся практике, и придерживаются. При этом, как отмечалось выше, и пользователи, и провайдеры попадают под юрисдикцию страны пребывания в связи с имущественными отношениями, исполнением договорных обязательств, финансовой, налоговой отчетностью и т. д. Но содержание их деятельности по передаче информации на транспортном и сетевом уровнях практически бесконтрольно.

Сегодня эта деятельность контролируется только Интернет сообществом, рынком телекоммуникационных услуг и регламентирующими организациями. Т.е. сложившаяся практика не предусматривает контроль со стороны государства, на территории которого часть сети и ее оборудования находится. При этом многие функции регулирования остаются под контролем одного государства, создавшего в свое время сеть Интернет. Например, корпорация ICANN осуществляет распределение адресного

пространства и доменных имен и поддержание системы DNS-серверов по всему миру (это можно рассматривать, как выдачу паспортов всем жителям Земли только под управлением иммиграционных служб США).

Но поскольку государство должно отвечать за преступные действия, совершаемые с его территории [9], оно должно обладать возможностями предотвратить или пресечь такие действия. В существующих транспортных системах государство, как правило, способно регулировать и контролировать и пути коммуникаций, и обеспечивающее их оборудование, и эксплуатирующие их компании, а также фильтровать трафик на границах (таможни, паспортный контроль, антитеррористический контроль, ветеринарный контроль и т.п.). В отношении же глобальной сети такая практика пока не сложилась.

Если подытожить перечисленные выше особенности сети, опыт эксплуатации различных транспортных систем (и отчасти систем связи) и предложения по технической реализации ряда новых функций и свойств, то очевидна необходимость:

1. формулировки в соответствии с национальным законодательством следующих требований, предусматривающих повышение надежности и безопасности информационной транспортной сети:

1.1. сертификация аппаратного и программного обеспечения КВИИ;

1.2. расширение систем регистрации на КВИИ;

1.3. резервирование КВИИ;

1.4. мониторинг функционирования сети;

1.5. устранение анонимности;

2. обеспечения контроля со стороны государства за текущим функционированием сети, находящейся на его территории;

3. подготовки резервных технических, информационных и организационных структур для поддержания работоспособности, мониторинга и управления сетью;

4. создания международных органов по сертификации, управлению регламентацией, систематизацией технических требований и расследованием инцидентов сети;

5. заключения международных соглашений, которые определяют не только общие правила и регламенты, но и гармонизируют национальные законодательства и правила взаимодействия стран между собой и существующими международными организациями;

6. заключения соглашений трансграничного обмена трафиком, предусматривающих более гибкое управление им, чем в существующих протоколах (BGP).

Литература

1. Clarke, Richard A. *Cyber War*, HarperCollins (2010)
2. The Russia− U.S. Bilateral on Cybersecurity− Critical Terminology Foundations, Issue 2
3. Стрельцов А.А. «Основные направления прогрессивного развития международного права вооруженных конфликтов», МГУ им. М.В.Ломоносова 2014. http://iisi.msu.ru/articles
4. «В поисках кибермира». Международный союз электросвязи и Всемирная федерация ученых. Geneva 2011. (Перевод на русский В.Бритков, В.Цигичко и др.)
5. Егизаров В.А. Транспортное право: Учебник для вузов. (3-е изд., стер.) — М.: ЗАО Юстицинформ, 2005.
6. Международные правила предупреждения столкновений судов в море, МППСС-72
7. Конвенция о Дорожных Знаках и Сигналах 1968 года http://www.unece.org/fileadmin/DAM/trans/conventn/signalsr.pdf
8. Европейское Соглашение, дополняющее Конвенцию 1971 года http://www.unece.org/fileadmin/DAM/trans/conventn/11-E-ECE-813r.pdf
9. The Tallinn Manual on the International Law Applicable to Cyber Warfare. General editor Michael N. Schmitt. Cambbridge University Press 2013.
10. Katharina Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn 2013
11. W32.Stuxnet Dossier. Nicolas Falliere, LoamO Murchu, Eric Chien. Symatiec Security Response. Version 1.4 (February 2011)

P.L.Pilyugin, A.A.Salnikov
Moscow State University
Institute of Information Security Issues

Prospects of application of international legal norms in cyberspace

The applicability of international law in cyberspace

In research and analysis of legal standards application for information security and legal regulation of cyberspace most attention is focused on the extension to cyberspace of the fundamental principles (humanitarian, non-proliferation, property, freedom of speech, protection of the individual, etc.) and the principles of international law enshrined in the UN Charter [1–3].

Another approach to research of legal regulation in cyberspace is based on the methods similar to the regulation of outer space, airspace and Antarctica, etc. [4]

And such analogies are not always correct. The main reason is that, although the abovementioned objects pertain the activities of mankind (otherwise there wouldn't have been such norms) the degree of their use is relatively low in comparison with the overall human activity. Cyberspace, on the contrary, affects almost all spheres of activity. Such an approach could be valid in cyberspace 20–30 years ago, followed by the development of «cyberlaw» and its division into different sections and directions with the development of the use of cyberspace. But presently the problem has become complicated to the extent that to regard this space as a whole is reasonable only from a philosophical point of view, while practice requires much greater detail.

What we now call cyberspace is essentially a superstructure built upon the sprawling data transmission infrastructure, upon the Internet. Therefore, the most popular approaches are the ones that involve representation of cyberspace foundations — the Internet, as a communications and transport system [4, 5].

In general, the Internet — is definitely a communication system — in terms of both its purpose and the social impacts, which, for example, communication systems have had on the society (primarily radio and television). However, the Internet is not just a communication network, but a computer network, a packet data network, and it is much more complicated, but also more flexible and versatile. In fact, it is a further evolution of communication systems, which requires the

development of appropriate standards and regulations; and the rapid development of packet data network — of the Internet, resulted in a situation where the rules of the previous communication systems are not adaptable to network structure.

However, if we recall that the Internet was created specifically as a transport medium, as a packet data network (IP data packets), and all these functions have already become an individual industry, we can see that the current economic practice is consistent with the activities of operators of non-information transport systems (shipping, aviation, railway and other transport companies). Following this line of reasoning, one can try to use the principles of legal regulation and security, developed over the many years of practice of non-information transport systems in the information infrastructure and use the methodology, approaches and practice of the complex and diverse transport law [5] and the transport regulatory guidelines [6–8] to find legal solutions related to a more detailed representation of the Internet and cyberspace.

Multilayer model of the global network

To simplify the issues in question, a multilayer ISO/OSI model, or a simple TCP/IP model (which is the basis of the Internet) is used in the analysis of the global Internet. Let's examine these layers using the abovementioned approach of comparing the Internet to different transportation systems.

Data link layer — these are real-world objects: fiber optics, satellites, twisted pair wires, simplest switches, etc. and the rules of their interaction.

In accordance with the proposed analogy, we can mention as an example the roads or railways with their functional devices (arrows, substations, etc.). This example may also include (with regard to their specific features) sea and river routes, air space for air traffic, and oil and gas pumping infrastructure. They all are physical material objects (or environments), which are regulated under national and international legislation and regulation rules. These physical carriers' regulators are, in particular, the International Telecommunication Union and others.

Network layer — is a layer of interaction between all these communication lines, and it also has physical devices, which for convenience are combined with the equipment of the physical (and the next, transport) layer — most notably, routers and switches.

By analogy with the preceding layer, here we can consider both vehicles and means of traffic control. For the railways there are locomo-

tives, carriages, traffic control systems and so on. It is easy to draw an analogy with the other forms of transport. All of this includes not only logical constructs and organizational structures, but also physical material objects. And being the material objects, they must be regulated by national and international legislation and specific regulatory guidelines. Today such specialized regulators are, in particular, ICANN, IANA and others.

Transport layer — a layer of more complex protocols, which facilitate network information exchange between different hosts, devices, applications, servers, and personal computers (or rather between their components responsible for information exchange).

We provide the following examples as an analogy: logistics, organization of cargo and passenger traffic between stations, terminals, ports, airfields, etc. All of this also includes not only organizational structures, but physical material objects as well. And being the material objects, they must be regulated by national and international legislation and regulatory guidelines. Today such regulators historically are ICANN, IANA and others.

Application layer — in fact this is the cyberspace where people and their software interact (in a certain sense it is already an artificial intelligence). To facilitate this interaction they require personal computers (or other devices of human interaction with the network) and servers, etc.

Applying the same analogy, we can consider exchange of goods between organizations, people, and transportation as such. Not only quantity is important here, but also the content: specific types of goods, migration, etc. All of this should also be regulated by national and international legislation. At this layer, there are also services which enhance the convenience of interaction with the transport system. In conventional transport systems these services include transport agencies, catering services, luggage processing system, and so on. Regarding the Internet, an analog is a more convenient network resources naming system — Domain Name System (DNS) and infrastructure information database (whois service). Their regulatory guidelines have been historically introduced and supported by the same regulators (ICANN, RIPE, and others).

From the abovementioned it is evident that the issue of network regulation of the cyberspace concerns primarily the network and transport layers. Application layer is of interest in terms of services that enable and «govern» the network and transport layers — for example, DNS, and infrastructure information database, in the other cases you can try to draw upon the existing rules. Here we consider the issues

of network security, based on the proposed approach (on the network and transport layers).

Special aspects of network security

When people talk about network security, it is understood as information security pertaining to a global network, to the elements of its network, transport and partially application layer and, above all, to the elements of critical information infrastructures (CII).

Security of network and transport layers implies: availability and integrity in information exchange, and in some cases, protection of data traffic and network controlling information (confidentiality). From the standpoint of network and transport layers, even if we do not consider the characteristics of different types of network attacks, it may be noted that the assurance of availability, spoofing resistance and confidentiality is related not only to destruction, interception, or injection of malicious traffic, but also to the issues of addressing and traffic management: routing and maintenance of the domain name system as a whole [10].

An architecture ideology of a global network suggests that it is a coherent association of individual networks — autonomous systems of the Internet (interaction between which is based on specific protocols), and this ensures high survivability and reliability of the network if the rules of interworking are fully complied with. However, the regulations are not always accurately and strictly followed, and they are deliberately broken in case of illegal actions (in military or criminal purposes), and communication protocols as such require development and refinement.

Another aspect is that attacks on the elements of the network are carried out through the network itself, through its network and transport layers [10]. If you apply the abovementioned analogy for these layers — these are attacks on the elements of the transport infrastructure: roads, bridges, stations, ports, ships, etc. (which have repeatedly happened in the world). Moreover, it is assumed that the source of the attack is a priori allowed to this infrastructure, and limited only by its regulations.

Another important aspect of network attacks is that it is easier to carry them out from the position of the provider (i.e. a position where there a direct access to network elements is available) or other direct participants in this activity, and it is essential for the attacks on routing systems or DNS. If you apply the previous analogy, we can say that the source of the attack is not only allowed to this infrastructure, but is its owner or a moderator, i.e. has almost limitless potential for its use.

Moreover, as mentioned above, all information exchange activities — is a trade in IP-traffic, and if it were not for an economic stimulus, the network would cease to exist. The main beneficiaries here are the providers engaged in peering and Internet traffic transit, and through them and the other network users profit is gained by equipment manufacturers. Regulatory authorities and partly different content providers such as Google, Facebook, and others — all live off these funds (however, this is related to the application layer, where there are also other financing sources). It is quite clear that all beneficiaries and other associated entities are interested in ensuring security and reliability of the network (otherwise the service will not be in demand). But this applies only to conditions where it is possible to get these benefits! Indeed, in any case of violation of normal economic activity due to external (revolution, martial law, nationalization, bankruptcy and so on) or internal causes none of the abovementioned organizations have an incentive to maintain the reliability and security of the network. The only interested parties are the users of the network (individuals, companies, government agencies).

Investigation and objectification of facts of network attacks

Investigation of possibilities to prevent, counter and investigate such network attacks is obstructed by the difficulty of their detection and attribution.

Firstly, it is difficult to determine whether the event was a flaw in design and software programming, or there was an actual computer attack. The fact is that any software has errors, the consequences of which could be catastrophic. There are enough examples of real disasters with a large number of casualties or huge economic losses caused by software errors, the source of which were design or programing flaws rather than cyberweapons or backdoors. All this requires a careful study of software code as a part of incidents analysis, and, in the absence of human-readable source code, this task is incredibly difficult and is comparable in complexity to creation of similar software.

Secondly, it is necessary to identify the source of the attack. In the well-known Stuxnet cyberattack, the alleged involvement of the United States and Israel in creation of the code has not been proved [11], although it is sometimes possible to detect the source of network DDOS-attacks, which are executed constantly on the network. Typically, they are conducted by hacker groups and not by cybertroops of nation-states. And everything is much more complicated in case of targeted attacks. The fact is that all of the existing «intrusion detec-

tion» systems actually detect only characteristics of an action, similar to intrusion or changes in the system, and the analysis of the actions, changes in the system and the machine code is performed by specialists. Furthermore, when the intrusion is detected significantly late, there remains no log data, and to determine the source it becomes necessary to analyze the machine code of embedded programs — and creators of such programs rarely leave autographs.

As it is evident from the abovementioned issues associated with the identification of the attack, technical means alone will be insufficient to determine the cause and origin, attribute the evidence of the criminal use of ICTs. For each such incident it will be necessary to conduct an investigation to determine its nature and to secure the obtained evidence in case the event is recognized as a criminal activity.

The same approach is used in existing transport systems. This is true not only with regard to international commissions, which investigate major air, rail or sea disasters, but also in cases of missing goods search, traffic disturbance, recovery of compensation for losses attributable to the carrier, etc. If the cause of the incident is not obvious, the work of such commissions usually starts with collection and verification of information on personnel qualifications and the quality of vehicles, their maintenance, inspections, certification, etc., as it allows not only to identify the possible causes of the incident, but also to create a basis for further work.

In case of such investigations, the correct attribution of network attacks requires, besides the arrangements for such investigations carried out by authorized personnel, it is necessary to envisage the requirements for the software that will be examined:

- software must be installed (purchased) officially;
- software must be signed by a trusted developer certificate;
- the developer should store (or hand over) the source code of the installed software for further analysis;
- all software changes (improvements, modifications, bug fixes) must be signed, and their source code — stored.

Such software requirements can be considered a certification of software that should be installed at information infrastructure nodes that can be targets of aggression and must be protected. On a side note, the use of uncertified equipment and transport routes constructed with violations of regulations has long been prohibited in existing transport systems, and it doesn't matter who the manufacturer was (Boeing, Airbus or TU).

Another important factor in attribution of facts of network attacks — is elimination of anonymity. In existing transport systems, where the

consequences of criminal acts can be significant (air, rail, maritime transport), no one has been traveling incognito for a long time, and only goods of the named customers are being transported. All information is recorded in individual tickets and consignment notes. However, anonymity still exists in public transportation or with regard to some postal items, but the cause of this is not the desire to preserve anonymity, but the complexity of capturing information for mass transportation or mail. In any case, other means of capturing information are used here, namely video surveillance systems in public transport, public places, etc.

Similar approaches can be used for global net users. This is not about sending a photo of the user with each of IP-packet he sends. But ISPs, in order to receive their payment, conclude service contracts with individuals and legal entities. More so, many content providers already use mobile devices as a means of user authentication or as payment terminals. That is, the implementation of authentication of any entity that interacts with a global network is technically feasible, and the results of such authentication should be made available only in case of carrying out an investigation, and this will make it possible not to infringe the right to commercial confidentiality or privacy.

Various means of registration are the most important source of information during investigations. In conventional transport systems, in addition to control information database, there are black boxes, which capture information of basic events taking place on board of the vehicle.

In the case of investigation of network attacks such information is often unavailable. This is primarily due to the fact that the number of events, occurring in the network, is too great, and either the registration systems are not able to store such quantities of information, or it becomes too expensive. Here it is appropriate to make three observations. Firstly, the registration systems are used for different purposes and for safety reasons they store redundant information — separation and storage of the most important information will make it possible to decrease the volume of stored data and to increase the time of its storage. Secondly, the most technologically complicated systems in terms of registration are the backbone nodes, where electronic equipment has already fallen behind the speeds provided by fiber-optic communication lines. In this case, we can recommend distributing the function of registration among slower nodes. Finally, thirdly, the transition to IPv6 makes it possible to include additional information in the «carrier vehicles» of the network, even though it will result in overhead costs increase — but security is never free of costs.

Prevention of Network Attacks

To ensure security it is more effective not just to detect and identify the sources of network attacks, but also to prevent them, to avoid possible negative effects.

In existing transport systems it is achieved by:

- terms and conditions of transportation services;
- transport network rules of operation;
- standards for vehicles and routes;
- introduction of administrative and criminal penalties for violation of these rules and regulations.

In the information network the function of such rules and regulations is exercised by various ISOs, RFCs and users connection rules. However, neither RFCs or ISOs have legal force (unless they are duplicated by a national standard — for the Russian Federation it is GOST). I.e. they are «de facto» standards and regulations, which are used according to an established practice. At that, as noted above, both users and service providers fall under the jurisdiction of the host country with regard to property relations, contractual obligations, financial and tax reporting, and so on. But the substance of their information transfer activities on the transport and network layers is virtually unchecked.

As of today, this activity is controlled only by the Internet community, telecommunication services market and regulatory organizations. I.e. the current practice does not provide for control by the country in which jurisdiction a part of the network and its equipment is located. This being said, many regulatory functions are controlled by a single country which at the time created the Internet. For example, ICANN distributes address space and domain names and carries out maintenance of DNS-servers worldwide (this can be considered as the issuance of passports to all inhabitants of the Earth only by US immigration services).

But because the State should be responsible for the criminal acts perpetrated from its territory [9], it should be able to prevent or terminate such actions. With regard to existing transport systems, the States, as a rule, are able to regulate and control communication lines, enabling equipment and their operators, and to filter traffic at the borders (customs, passport control, anti-terrorism control, veterinary control, etc.). With regard to the global network, such practice has not been developed yet.

If we sum up the above-mentioned aspects of the network, operating history of different transport systems (and partly of communication

systems) and the proposals for technical implementation of a number of new functions and features, there is an evident need to:

- formulate in accordance with the national legislation of the following requirements, which provide for increased reliability and security of the information transport network:
  - ◊ certification of CII hardware and software;
  - ◊ expansion of the registration systems to CII;
  - ◊ CII backup;
  - ◊ network performance monitoring;
  - ◊ elimination of anonymity;
- facilitate control by the State of the current operation of the network located in its territory;
- prepare back-up technical, information and organizational structures in order to maintain efficiency, monitoring and network management;
- establish international bodies for certification, regulations management, technical requirements systematization and investigation of network incidents;
- establish international agreements that define not only general rules and regulations, but also harmonize national legislation and rules of interaction between governments and the existing international organizations;
- establish agreements on cross-border traffic exchange, which provide for the more adaptive control over it than the existing protocols (BGP).

References

1. Clarke, Richard A. *Cyber War*, HarperCollins (2010)
2. The Russia — US Bilateral on Cybersecurity — Critical Terminology Foundations, Issue 2
3. A.A.Streltsov «Focal Areas in Progressive Development of the International Law of Armed Conflict» (in Russian)(«Основные направления прогрессивного развития международного права вооруженных конфликтов»), Moscow State University, 2014. http://iisi.msu.ru/articles
4. The Quest for Cyber Peace. The International Telecommunication Union and the World Federation of Scientists. Geneva 2011.
5. V.A.Egizarov Transport Law: Textbook for universities. (Транспортное право: Учебник для вузов. М.: ЗАО Юстицинформ), 2005.
6. International Rules for Preventing Collisions at Sea, COLREGs, 1972
7. Convention on Road Signs and Signals, 1968 http://www.unece.org/fileadmin/DAM/trans/conventn/signalsr.pdf

8. European Agreement Supplementing the Convention on Road Traffic opened for Signature at Vienna on 8 November 1968 http://www.unece.org/fileadmin/DAM/trans/conventn/11-E-ECE-813r.pdf

9. The Tallinn Manual on the International Law Applicable to Cyber Warfare. General editor Michael N. Schmitt. Cambridge University Press in 2013.

10. Katharina Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn 2013

11. W32.Stuxnet Dossier. Nicolas Falliere, Loam O. Murchu, Eric Chien. Symatiec Security Response. Version 1.4 (February 2011)

Томас Ламанаускас, Деспоина Сарейдаки, Преетам Малур

Международный союз электросвязи

Защита критически важной инфраструктуры: многоуровневый подход

A. Введение

За последнее десятилетие Интернет стал неотъемлемой частью каждой из сторон нашей жизни, и его значимость продолжает возрастать. В настоящий момент более 40%[1] населения мира являются пользователями Интернета. Обеспечение доступом остальной части мира является одной из главных целей МСЭ. Однако важно, чтобы эта цель была достигнута сбалансированным образом.

Несмотря на значительную пользу, Интернет также становится источником существенных рисков. По мере расширения подключенности и роста нашей зависимости от Интернета, киберинциденты становятся более частыми, изощренными и оказывают значительное экономическое и социальное воздействие. Более того, совершающие их акторы демонстрируют высокую адаптивность при обходе различных мер защиты. В своем докладе 2013 года об экономических последствиях киберпреступности компания McAfee привела оценку, что вероятные ежегодные потери глобальной экономики от киберпреступности составляют более 455 миллиардов долларов. Рост этого явления также показан в ряде различных отчетов, посвященных описанию общей картины глобальной киберугрозы. Например, отчет об угрозах Интернет-безопасности 2015 корпорации Symantec указал на 23% прирост количества утечек данных в 2013–2014 годах.

Поскольку в ближайшие годы большая часть роста использования ИКТ будет приходиться на развивающиеся страны, ожидается, что их уязвимость к киберрискам в ближайшие годы также окажется в центре внимания.

[1] См. публикацию ITU's ICT Facts and Figures, 2015 года

B. Критически важные инфраструктуры в цифровую эпоху

Критически важная инфраструктура включает в себя все секторы, которые считаются основополагающими для социально-экономического благополучия страны. Сектора критически важной инфраструктуры зависят от такой физической инфраструктуры как здания, дороги, заводы и трубопроводы. Эти сектора также во всё большей степени зависят от киберпространства и информационных и коммуникационных технологий (ИКТ), которые лежат в его основе, что в совокупности в настоящее время классифицируется как критически важная информационная инфраструктура. Она обеспечивает функционирование и управление критически важными секторами и их физическими активами. Поэтому её уровень безопасности имеет первостепенное значение для укрепления доверия, так как отсутствие уверенности в использовании ИКТ может мешать повседневной жизни, а также коммерческим операциям и работе правительства[2].

Учитывая сильную зависимость современной промышленности от ИКТ, киберинциденты затрагивают широкий спектр секторов критически важной инфраструктуры, а наибольшему риску[3] подвержены горнодобывающая промышленность, торговля, производство, коммунальные услуги и государственное управление.

C. МСЭ и кибербезопасность[4]

МСЭ является специализированным учреждением ООН по вопросам ИКТ. Его история насчитывает 150 лет и охватывает на этом промежутке времени широкий спектр информационных и коммуникационных технологий. Безопасность телекоммуникаций всегда была одним из ключевых направлений деятельности МСЭ, однако с появлением и распространением информационных технологий возникли новые риски, для которых потребовался более скоординированный ответ.

На Всемирной встрече на высшем уровне по вопросам информационного общества (ВВУИО), состоявшейся в 2003 и 2005 году, МСЭ была поручена роль единственного исполнителя пункта С5 плана мероприятий ВВУИО — «Укрепление доверия и безопасности при использовании ИКТ»[5]. В продолжение этой работы МСЭ

---

[2] См. ITU National Cybersecurity Strategy Guide (2011)

[3] См. Symantec Internet Security Threat Report, Volume 20, April 2015

[4] Новая информация о деятельности МСЭ в области кибербезопасности доступна по адресу: www.itu.int/cybersecurity

[5] См. Женевский План действий (2003)

разработал Глобальную программу кибербезопасности (ГПК) в 2007 году, которая представляет собой международный механизм сотрудничества в области кибербезопасности. ГПК построена на пяти стратегических областях работы (правовые меры, технические и процедурные меры, организационные структуры, наращивание потенциала, международное сотрудничество), которые до сих пор определяют работу МСЭ. Государства-члены МСЭ усилили роль организации, приняв ряд резолюций, касающихся разработки, а также стандартизации работы организации, в частности, признав риски, которым подвержена критически важная инфраструктура.

1. Актуальные мероприятия Отдела развития МСЭ (ITU-D)

a. Предоставление руководящих указаний в разработке Национальной стратегии по кибербезопасности

В связи с возрастанием рисков в киберпространстве и в рамках своей работы по наращиванию потенциала, МСЭ разработала Руководство по национальным стратегиям кибербезопасности, где большое внимание уделено вопросам, которые страны должны учитывать при разработке или пересмотре национальных стратегий в области кибербезопасности, особенно по отношению к защите критически важной национальной инфраструктуры.

Поскольку возможности государств, потребности и угрозы различны, странам рекомендуется использовать национальные ценности и интересы в качестве основы для своих стратегий. Этот подход обоснован тем, что культура и национальные интересы часто влияют на восприятие риска и относительную успешность защиты от киберугроз. Кроме того, стратегия, основанная на национальных ценностях, вероятно, получит поддержку таких заинтересованных сторон, как органы юстиции и частный сектор[6].

Руководство МСЭ по национальным стратегиям кибербезопасности содержит предложения по конкретным действиям, которые должны быть предприняты странами для противодействия общим киберугрозам и защиты критически важной национальной инфраструктуры. Руководство использует пять столпов Глобальной программы кибербезопасности (ГПК) как отправную точку, которую государства должны учитывать при принятии соответствующих мер.

---

[6] См. Руководство МСЭ по национальным стратегиям кибербезопасности (2011)

b. Создание национальных команд реагирования на компьютерные инциденты (CIRTs)

Рост изощренности, частоты и опасности киберугроз требует создания формальных механизмов и организационных структур для мониторинга, предупреждения и реагирования на инциденты. Как указано в Руководстве МСЭ по национальным стратегиям кибербезопасности, Национальные команды реагирования на компьютерные инциденты являются ключевыми элементами Национальных стратегий кибербезопасности и первой линией обороны против любых потенциальных угроз, которые могут представлять опасность для критически важных инфраструктур страны. В задачи Национальных команд реагирования на компьютерные инциденты, среди прочего, входит:

I. Оказание поддержки при реагировании на инциденты;

II. Осуществление раннего предупреждения и оповещения;

III. Координация связи и содействие обмену информацией между заинтересованными сторонами;

IV. Разработка стратегий по смягчению последствий и реагированию и координация реагирования на происшествия;

V. Обмен данными и информацией об инциденте и соответствующих ответных действиях;

VI. Публикация передового опыта реагирования на инциденты и советов по профилактике;

VII. Координация международного сотрудничества по киберинцидентам.

В настоящее время во всем мире существует 102 Национальные команды реагирования на компьютерные инциденты. МСЭ в рамках своей программы Национальных команд реагирования на компьютерные инциденты работает над тем, чтобы заполнить оставшиеся пробелы, и оказывает помощь государствам-членам в три этапа:

I. Рассмотрение: Оценка готовности стран к созданию Национальных команд реагирования на компьютерные инциденты;

II. Реализация: Оказание помощи странам в вопросах планирования, ввода в действие и эксплуатации Национальных команд реагирования на компьютерные инциденты, а также повышение компетентности по эксплуатационным и техническим аспектам;

III. Киберучения: Организация практических киберупражнений в различных регионах для приведения в готовность вновь созданных Национальных команд реагирования на компьютерные инциденты, повышения уровня их опыта и развития взаимодействия между ними.

На сегодняшний день (июнь 2015 г.) МСЭ завершил оценку 67 стран и продолжает рассмотрение ещё двух. Национальные команды реагирования на компьютерные инциденты были введены в действие в 11 странах, и в четырех странах этот процесс продолжается. МСЭ также организовал 11 киберупражнений, в которых приняло участие более чем 100 государств. Ежегодно планируется проведение большего числа киберупражнений.

c. Развитие кибербезопасности в наименее развитых странах

По мере того как не подключенные ранее части мира выходят в сеть, неизбежным становится воздействие на них киберрисков, также возрастает риск, что они станут источником кибератак. Тем не менее, в то же время они находятся в выгодном положении, поскольку имеют возможность учиться у более опытных стран и вооружиться необходимыми инструментами на ранней стадии.

Проект МСЭ «Укрепление кибербезопасности в наименее развитых государствах» направлен на оказание помощи наименее развитым странам в расширении их возможностей, потенциала, готовности, умений и знаний в области кибербезопасности. Помимо наращивания человеческого потенциала, проект также направлен на обеспечение наименее развитых государств необходимыми базовыми технологиями и связанными с ними инструментами для оказания помощи в проведении мероприятий по обеспечению безопасности их киберпространства.

Проект, который включает в себя в общей сложности 49 стран, на сегодняшний день (июнь 2015г.) был реализован в четырех странах, и находится на разных этапах планирования/реализации в еще 15 странах.

d. Глобальный индекс кибербезопасности (GCI)

Пробелы в обеспечении национальной кибербезопасности вызывают сильные риски для основных компонентов жизненно важных сетей снабжения государства (водо- и электроснабжение, телекоммуникации, банковский сектор и т.д.) и, следовательно, для социально-экономической стабильности. Кроме того, слабость механизмов реагирования на киберугрозы в одной стране фактически может быть использована злонамеренными акторами для осуществления нападений на другие государства.

МСЭ осуществляет проект «Глобальный индекс кибербезопасности» (GCI) чтобы определить уровень активности государств в

обеспечении кибербезопасности на пяти основных направлениях Глобальной программы кибербезопасности: правовых мерах, технических и процедурных мерах, создании организационных структур, наращивании потенциала, международном сотрудничестве.

Эта инициатива в целом направлена на помощь странам в определении областей развития кибербезопасности, а также на мотивацию действий для улучшения своего рейтинга — тем самым помогая повысить общий уровень кибербезопасности в мире. На основе собранной в рамках программы информации демонстрируется деятельность одних государств, так что другие страны могут внедрить отдельные аспекты этих практик, подходящие их национальной среде. Целью этой работы является гармонизация практик и развитие глобальной культуры кибербезопасности.

Результаты Глобального индекса кибербезопасности 2014 года были опубликованы вместе с рядом профилей «киберблагополучия»[7], которые являются реальным фактическим отображением мер, предпринятых или планируемых на уровне государств для повышения кибербезопасности. Это упражнение призвано помочь государствам лучше оценить их состояние кибербезопасности и дать им возможность учиться у других государств. Разрабатываемая в настоящее время очередная итерация Глобального индекса кибербезопасности будет охватывать большее количество партнеров, иметь более широкий размах и включать в себя большее число консультаций со всеми заинтересованными сторонами.

2. Актуальные мероприятия Отдела стандартизации МСЭ (ITU-T)

Отдел стандартизации МСЭ способствует развитию критически важных стандартов, которые позволяют создавать более безопасные и надежные ИКТ-устройства. 17-я исследовательская группа по безопасности содействует интенсивной работе по технической стандартизации в промышленности, среди правительственных администраций, научных и научно-исследовательских учреждений, а также других субъектов, таких как партнерские организации разработки стандартов, форумы и консорциумы. Это создаёт условия для достижения международного консенсуса в отношении различных стандартов кибербезопасности.

[7] См. сайт МСЭ: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

17-я исследовательская группа Отдела стандартизации МСЭ выпустила более 330 рекомендаций, многие из которых связаны с кибербезопасностью. На повестке дня стандартизации в области кибербезопасности стоят следующие темы: кибербезопасность, безопасность облачных вычислений, онлайн-аналитика, безопасность Интернета вещей, безопасность интеллектуальных систем энергоснабжения, безопасность программно-конфигурируемых сетей, безопасность сотовой связи, безопасность интеллектуальных транспортных систем, технические меры борьбы со спамом, управление идентификацией пользователей, конфиденциальность и безопасность личной информации, инфраструктура сертификации открытых ключей, архитектура безопасности, управление информационной безопасностью, телебиометрика, защищенная электронная почта, и безопасность приложений.

3. Партнерство и сотрудничество

Принимая во внимание то, что многогранный характер кибератак требует специальных знаний и действий на разных уровнях (как виртуальных, так и физических), становится ясно, что кибербезопасность не может обеспечиваться усилиями только одного актора. В этом отношении МСЭ тесно сотрудничает с рядом других межправительственных организаций, частных компаний и научных сообществ, чтобы обеспечить экспертную поддержку своим странам-членам по вопросам кибербезопасности. Некоторые примеры включают в себя:

a. Глобальный форум экспертного потенциала по кибервопросам (GFCE)

Во время Глобальной конференции по киберпространству, состоявшейся в Гааге, Нидерландах 16–17 апреля 2015 года, был создан Глобальный форум экспертного потенциала по кибервопросам. Этот форум включает 42 учредителя, в том числе МСЭ. Всего в рамках форума было организовано 15 инициатив сотрудничества, и МСЭ, наряду с Нидерландами, Организацией американских государств (ОАГ) и Microsoft, является со-инициатором «Инициативы развития групп реагирования на инциденты, связанные с компьютерной безопасностью». Целью этой инициативы является предоставление членам Глобального форума платформы для помощи в развитии новых и существующих команд реагирования на инциденты компьютерной безопасности.

b. Распространение докладов о киберугрозах среди членов МСЭ

В соответствии со своей давней традицией государственно-частного партнерства, МСЭ сотрудничает с Symantec и Trend Micro в предоставлении регулярных докладов о киберугрозах своим государствам-членам, повышая осведомленность о текущем состоянии кибербезопасности и таким образом позволяя государствам принять надлежащие меры.

c. Механизмы сотрудничества ООН

В ноябре 2013 года Координационным советом руководителей системы ООН было одобрено создание в масштабах ООН общих принципов по кибербезопасности и киберпреступности. Они разрабатывалась 35 учреждениями и органами ООН в течение трех лет, а МСЭ и Управление Организации Объединенных Наций по наркотикам и преступности (УНП ООН) осуществляли координацию усилий. Итоговый документ призван обеспечить продвинутую координацию между подразделениями ООН, которые предоставляют ответы на запросы государств-членов в области кибербезопасности и киберпреступности в соответствии со своими ролями и полномочиями.

По просьбе Генерального секретаря Организации Объединенных Наций г-на Пан Ги Муна, и опираясь на одобренные в масштабах ООН общие принципы кибербезопасности и киберпреступности, в 2014 году, в сотрудничестве со всей системой учреждений ООН, был сформулирован внутрисистемный план ООН по координации вопросов кибербезопасности и киберпреступности. Этот план предназначен для направления деятельности системы учреждений ООН по внутренней координации в области кибербезопасности и киберпреступности.

d. Заключение — необходимость многоуровневого подхода

Для достижения эффективного уровня кибербезопасности во всём мире необходимо использовать многоуровневый ответ на киберпроблемы.

Это означает, что на уровне государств деятельность должна быть направлена на разработку и реализацию эффективных национальных стратегий, политики и законодательства, развитие необходимых возможностей реагирования, а также наращивание потенциала и развитие обучения. Однако такие меры должны быть дополнены гармонизацией законодательства и учетом пере-

дового опыта на региональном уровне, а также международными механизмами сотрудничества и обмена информацией.

МСЭ стремится предоставить всю необходимую государствам помощь для достижения гармонизированной и эффективной среды кибербезопасности, которая должным образом противодействовала бы рискам, связанным с использованием ИКТ, и дала бы национальным экономикам возможность развиваться в отсутствии, насколько это возможно, постоянной угрозы, исходящей от киберпроблем.

Tomas Lamanauskas, Despoina Sareidaki,
Preetam Maloor

International Telecommunication Union

Protecting Critical Infrastructure: A multi-layered approach

A. Introduction

Over the last decade, the Internet has gradually become an integral part of every aspect of our lives and it continues to increase in importance. At the moment, Internet users constitute over 40%[1] of the world's population. Bringing the rest of the world online is one of ITU's primary commitments. However, it is important for this to be achieved in a sustainable manner.

Despite its enormous benefits, the Internet also brings significant risks. As connectivity is expanding and we grow to be more reliant on the Internet, cyber-incidents are becoming more frequent, complex and with significant economic and social impact. Furthermore, their actors demonstrate strong adaptability in bypassing the different protection measures. In its Report on Economic Impact of Cybercrime 2013, McAfee estimated that the likely annual cost to the global economy from cybercrime is more than $455 billion. The growth of the phenomenon is further demonstrated in a number of different reports aiming to capture the global cyber-threat landscape. For example Symantec's Internet Security Threat Report 2015 identified a 23% increase in data breaches from 2013 to 2014.

As most of the growth in the adoption of ICTs in the coming years will come from developing countries, their vulnerability to cyber-risks is also expected to come into a particular focus in the years to come.

B. Critical infrastructure in the digital era

Critical infrastructure comprises all sectors that are considered fundamental for the socio-economic well-being of a country. Critical infrastructure sectors rely on physical infrastructure such as buildings, roads, plants and pipes. Increasingly, these sectors also rely on cyberspace and the information and communication technologies (ICTs) that enable it, which is being classified as the critical information infrastructure (CII). The CII enables operation and control of the critical

[1] See ITU's ICT Facts and Figures, 2015 Edition

sectors and their physical assets. Therefore its security level is essential for building trust, as lack of confidence in the use of ICTs could hinder daily life as well as commercial and governmental operations[2].

Given the strong dependence of today's industry on ICTs, cyber-incidents have been affecting a broad range of critical infrastructure sectors, with mining, wholesale, manufacturing, utilities and public administration demonstrating the highest cyber-risk rates[3].

C. ITU and Cybersecurity[4]

ITU is the United Nations' specialized agency for ICTs with a history of 150 years covering a broad range of communication and information technologies along the way. The security of telecommunications has always been one of the key activities of the ITU, however with the emergence and proliferation of information technologies, new risks arose that needed a more coordinated response.

At the World Summit on the Information Society (WSIS) held in 2003 and 2005, ITU was entrusted the role of the sole facilitator for WSIS Action Line C5 on "Building confidence and security in the use of ICTs"[5]. As a follow-up, ITU developed the Global Cybersecurity Agenda (GCA) in 2007, which is an international framework for cooperation in the area of cybersecurity. The GCA is built upon five strategic work areas (Legal Measures, Technical & Procedural Measures, Organizational Structures, Capacity Building, International Cooperation) that shape ITU's work until today. ITU Member States further reinforced ITU's role by adopting a number of resolutions pertaining to the development, as well as standardization work of the organization, specifically recognizing the risks imposed on critical infrastructure.

1. Relevant activities of the ITU Development Sector (ITU-D)

a. Providing guidance in the development of National Cybersecurity Strategies

In view of the growing risks in cyberspace and as part of its capacity building work ITU developed a National Cybersecurity Strategy Guide, focusing on the issues that countries should consider when elaborating or reviewing national cybersecurity strategies, especially with regard to the protection of critical national infrastructure.

---

[2] See the ITU National Cybersecurity Strategy Guide (2011)

[3] See Symantec Internet Security Threat Report, Volume 20, April 2015

[4] For updated information on ITU's cybersecurity activities visit the ITU website: www.itu.int/cybersecurity

[5] See Geneva Plan of Action (2003)

As national capabilities, needs and threats vary, countries are recommended to use national values and interests as a basis for their strategies. The rationale behind this approach is that culture and national interests often influence the perception of risk and the relative success of defences against cyber-threats. In addition, a strategy rooted in national values is likely to gain support of stakeholders such as the judiciary and private sector[6].

The ITU National Cybersecurity Strategy Guide provides suggestions on specific actions to be undertaken by countries, in order to address general cyber-threats and protect critical national infrastructure. The Guide uses the five pillars of the Global Cybersecurity Agenda (GCA) as a starting point for governments to consider when taking appropriate measures.

b. Establishment of National Computer Incident Response Teams (CIRTs)

The growing sophistication, frequency and gravity of cyber-threats require formal frameworks and organizational structures for monitoring, warning and incident response. As explained in the ITU's National Cybersecurity Strategy Guide, CIRTs are key elements in a country's National Cybersecurity Strategy and the first line of defence against any potential threats that could present a hazard to a country's critical infrastructures. The role of a CIRT includes inter alia:

i. Provision of incident response support;

ii. Dissemination of early warnings and alerts;

iii. Facilitation of communications and information sharing among stakeholders;

iv. Development of mitigation and response strategies and coordinating incident response;

v. Data and information sharing about the incident and respective responses;

vi. Publication of best practices in incident response and prevention advice;

vii. Coordination of international cooperation on cyber-incidents.

Currently there are 102 national CIRTs worldwide. ITU has been working to fill the remaining gaps through its National CIRT programme, which provides assistance to its Member States in three stages:

i. Assessment: Evaluation of the preparedness of countries for the establishment of National Computer Incident Response Teams (CIRTs);

[6] See the ITU National Cybersecurity Strategy Guide (2011)

ii. Implementation: Assistance to countries with the planning, implementation, and operation of a CIRT, as well as capacity building on the operational and technical details;

iii. Cyber-drills: Organization of hands-on cyber-exercises in different regions in order to bring newly-established CIRTs up to speed, enhance their maturity and promote CIRT-to-CIRT cooperation.

To date (June 2015), ITU has completed assessments in 67 countries and two are still ongoing. CIRT implementations have been carried out in 11 countries, while they are still in progress in 4 countries. ITU has also organized 11 cyber-exercises, involving more than 100 countries, and more are planned every year.

c. Enhancing Cybersecurity in Least Developed Countries

As unconnected parts of the world go online, their exposure to cyber-risks becomes inevitable, together with the increased risk for them to become a source of cyber-attacks. However, at the same time they find themselves in an advantageous position as they have the opportunity to learn from more experienced countries and equip themselves with the necessary tools at an early stage.

ITU's project on "Enhancing Cybersecurity in Least Developed Countries (LDCs)" focuses on assisting LDCs to enhance their capabilities, capacity, readiness, skills and knowledge in the area of cybersecurity. Apart from human capacity building, the project is also geared towards providing the appropriate enabling technologies and related tools to assist LDCs in carrying out activities with regard to securing their cyberspace.

The project, which involves a total of 49 countries, has to date (June 2015) been implemented in four countries, and is at different stages of planning/implementation in 15 more countries.

d. The Global Cybersecurity Index (GCI)

Gaps in national cybersecurity efforts imply strong risks for crucial components of the country's vital supply networks (water, electricity, telecommunications, banking etc) and thus social and economic stability. Furthermore a country's weak response mechanisms to cyber-threats can actually be exploited by threat actors in order to launch attacks against further countries.

ITU is leading the Global Cybersecurity Index (GCI) project to measure the commitment of countries to cybersecurity in the five main areas of the Global Cybersecurity Agenda: legal, technical, organizational, capacity building, and national and international cooperation.

The overall aim of the GCI initiative is to help countries identify areas for improvement in the field of cybersecurity, as well as motivate them to take action to improve their ranking, thus helping raise the overall level of cybersecurity worldwide. Through the collected information, the GCI initiative illustrates the practices of others, so that countries can implement selected aspects suitable to their national environment, with the objective to harmonize practices and foster a global culture of cybersecurity.

The 2014 GCI results have been published together with a collection of Cyberwellness profiles[7], which are living and factual representations of measures undertaken or planned at country level to enhance cybersecurity. The purpose of this exercise is to enable countries to better assess their cybersecurity readiness and learn from their peers. The next iteration of the GCI is currently being elaborated and will encompass more partners, a wider scope and more consultations with all stakeholders.

2. Relevant activities of the ITU Standardization Sector (ITU-T)

ITU's standardization sector contributes to the development of critical standards that enable the creation of more secure and robust ICT devices. ITU-T Study Group 17 on Security facilitates intensive work on technical standardization among industry, government administrations, academia and research establishments, as well as other entities, such as partner Standard Development Organizations (SDOs), Forums and Consortia. This enables building international consensus on the various cybersecurity standards.

ITU-T Study Group 17 has produced over 330 Recommendations, many of which are related to cybersecurity. Topics on the cybersecurity standardization agenda have included: cybersecurity, cloud computing security, online analytics, Internet-of-Things security, smart-grid security, software-defined networking security, mobile security, Intelligent Transportation System security, anti-spam technical measures, identity management, privacy/PII, public-key infrastructure, security architecture, information security management, telebiometrics, secure e-mail, and application security.

3. Partnerships and Cooperation

Bearing in mind that the multifaceted nature of cyber-attacks requires specialized knowledge and action at different levels (both virtual

[7] See ITU Website: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

and physical), it is clear that cybersecurity cannot be achieved through the efforts of one actor alone. In this respect, ITU has been collaborating closely with a number of other intergovernmental organizations, private companies and academia to provide expert assistance to its Membership with regard to cybersecurity. Some examples include:

a. Global Forum on Cyber Expertise (GFCE)

During the Global Conference on Cyberspace (GCCS) held in The Hague, Netherlands on 16–17 April 2015, the Global Forum on Cyber Expertise (GFCE) was launched. This forum comprises 42 Founding Members, including ITU. Some 15 cooperation initiatives were launched within the framework of the GFCE, with ITU being the co-initiator of the "CSIRT Maturity Initiative", along with the Netherlands, Organization of American States (OAS) and Microsoft. The objective of the Cyber Security CSIRT Maturity Initiative is to provide a platform to GFCE members to help emerging and existing Computer Security Incident Response Teams (CSIRTs) to increase their maturity level.

b. Dissemination of cyber-threat reports to the ITU Membership

In line with its long tradition of public-private partnership, ITU has been collaborating with Symantec and Trend Micro on the provision of regular cyber-threat reports to its Member States, thus enhancing awareness on the current cybersecurity landscape and allowing countries to take proper measures.

c. UN-wide cooperation mechanisms

In November 2013, a UN-wide framework on Cybersecurity and Cybercrime was endorsed by the United Nations Chief Executives Board (CEB). This framework was developed by 35 UN agencies and bodies over the course of three years, with ITU and the United Nations Office on Drugs and Crime (UNODC) leading the coordination of the effort. The document aims to facilitate enhanced coordination among United Nations (UN) entities, in their response to concerns of Member States regarding cybersecurity and cybercrime, based on their respective roles and mandates.

Following a request by the United Nations Secretary-General, Mr. Ban Ki-moon, and building on the endorsed UN-wide framework on Cybersecurity and Cybercrime, a UN System Internal Coordination Plan on Cybersecurity and Cybercrime was formulated with the contribution of the entire UN System in 2014. This plan is designed to guide

internal coordination activities of the UN system organizations in the area of cybersecurity and cybercrime.

d. Conclusion — Need for a Multi-layered approach

In order for the world to achieve an effective level of cybersecurity, it is necessary to apply a multi-layered response to cyber-challenges.

This translates into a focus of action at the country level through the elaboration and implementation of effective national strategies, policies and legislation, development of the necessary response capabilities, as well as country-level capacity building and training. Such measures, however, need to be complemented by the harmonization of legislation and learning from best practices at the regional level, as well as international cooperation frameworks and exchange of information at the international level.

ITU is committed to provide all necessary assistance to countries in order to achieve a harmonized and effective cybersecurity environment, which would properly manage the risks involved in the use of ICTs and allow the national economies to grow, deprived, as much as possible, of the constant threat of cyber-challenges.

Сандро Болонья, Маурицио Мартеллини
Центр международной безопасности Университета Инсубрия (Италия)

Клаудио Калисти
Компания ASTER-TE (Италия)

ИКТ-системы для сложных инфраструктур: от технологий безопасности к решениям безопасности

1. Введение

Недавние примеры уязвимостей свидетельствуют о том, что модель безопасности 10–15 летней давности больше не соответствует современным вызовам, возникшим в результате повсеместного использования Интернета в каждой ИКТ-системе. Эта модель устарела и не масштабируема в условиях сегодняшних угроз ИКТ-системам. По мере того, как служащие, партнеры и клиенты начали вести дела удаленно через Интернет, модель безопасности на основе защиты периметра эволюционировала в сильно распределенную модель. Индустрия безопасности представила новые и улучшенные решения для противодействия каждой новой угрозе, появляющейся в этом сценарии. Все эти инструменты добавляют вре́менную ценность к общей безопасности предприятия, но они, в сущности, являются индивидуальными решениями безопасности, направленными против отдельных угроз. Они не являются производными от общей риск-ориентированной программы обеспечения безопасности предприятия, поэтому общие усилия, как правило, носят фрагментарный характер. Во многих случаях организациям приходится иметь дело с неполной информацией, поскольку имеющийся инструмент безопасности не может определить угрозу или опасность как таковую без корреляции с другими источниками данных. В ответ на изменяющийся спектр угроз были разработаны разнообразные технологии безопасности, но при этом не хватает методологии, на основе которой строится анализ контекста безопасности и впоследствии разрабатывается соответствующее решение. Деятельность, которая выглядит безвредной для одной части инфраструктуры, может быть определена как угроза после корреляции со всей остальной инфраструктурой.

2. Запланированная безопасность (Security-by-Design)

По определению Государственного департамента США[1]: «Запланированная безопасность» представляет собой концепцию, которая включает в себя безопасность на всех этапах и аспектах проектирования, строительства и функционирования предприятия. Безопасность рассматривается с точки зрения управления жизненным циклом, благодаря чему проектирование, создание и техническое обслуживание объекта осуществляется таким образом, чтобы обеспечить эффективность и продуктивность обеспечения безопасности. В начале этапа проектирования объекта посредством оценки уязвимостей и использования инструментов моделирования проект проходит испытания по всему спектру угроз. Проект изменяется в соответствии с выявленными проблемами, и последующие изменения в конструкцию оцениваются таким же образом на всем протяжении жизненного цикла системы.

По определению Национальных лабораторий SANDIA, главной целью запланированной безопасности является обеспечение выполнения задачи, в то время как уровень безопасности должен превышать возможности угрозы.[2] Таким образом, анализ безопасности должен проводиться на ранней стадии проектирования системы, и он должен обеспечить соответствующий уровень безопасности в течение всего времени выполнения задачи, т.е. на протяжении всего жизненного цикла системы. Безопасность критически важной инфраструктуры и безопасность ИКТ-систем не являются механически компонуемыми. ИКТ-системы могут считаться полностью безопасными, когда они являются автономными и все компоненты и цепи поставок соответствуют строгим требованиям, демонстрируя уязвимости при интеграции в реальные эксплуатационные условия (интеграция с другими компонентами общей социотехнической системы, т.е. другими ИКТ-системами и сетями, операторами, процедурами и методами работы). В случае с защитой критически важных инфраструктур, невозможно обеспечить безопасность ИКТ-систем без детального рассмотрения условий их эксплуатации с технической, архитектурной и операционной точек зрения. Это также связано

---

[1] http://www.state.gov/t/isn/rls/fs/186672.htm

[2] SANDIA REPORT, Security-by-Design Handbook, SAND2013-0038, January 2013, Albuquerque (US). http://prod.sandia.gov/techlib/access-control.cgi/2013/130038.pdf

с тем, что, хотя контроль над критически важными инфраструктурами и системами управления на самом деле осуществляется ИКТ-системами (в том числе телекоммуникации, компьютеры, программное обеспечение предприятия, межплатформное программное обеспечение, системы хранения, системы отображения и т.д.), они имеют такие ограничения как режим точного реального времени и обеспечения непрерывности, что делает невозможным использование многих обычных применяющихся в ИКТ контрмер (например, использование брандмауэра и антивируса, а также обновлений программного обеспечения).

В то время как изначально защита критических инфраструктур преимущественно обеспечивалась системами жизнеобеспечения, методы разработки парадигм запланированной безопасности остаются недостаточно разработанными. Чтобы быть эффективной, защита должна учитывать сложные взаимозависимости и взаимодействия, порождаемые соединением физической и ИКТ-инфраструктуры вместе с производственной деятельностью и операторами. Вместе они образуют системный объект с высоким уровнем требований безопасности. Эволюция и изменения в требованиях, нагрузках и других факторах окружающей среды приводят к необходимости комплексной замкнутой оценки конструкций и их работы. Кроме того, изменение ключевых показателей эффективности, например, иная оценка рисков, безопасности, пропускной способности и т.д., в различных условиях требует, по крайней мере, набора заранее выверенных сценариев работы. Такой многосторонний анализ существующих инфраструктур является основой их эффективного функционирования.

Одну и ту же критически важную инфраструктуру можно рассматривать с разных точек зрения[3]. Эти точки зрения можно считать размерностями трехмерного пространства: измерение компонент, измерение контрмер и измерение рисков (рис. 1).

Каждая точка пространства на рис. 1 представляет собой контрмеры, применяемые к компонентам системы для противодействия конкретной угрозе. В компонентном измерении критически важная инфраструктура разделяется на составные части, которые могут быть физическими или логическими. Соответственно, можно определить физическую и логическую архитектуру критически важной инфраструктуры.

---

[3] AIIC Piano di Sicurerzza dell'Operatore: Proposta di line guida operative (in Italian) http://www.infrastrutturecritiche.it/aiic/index.php?option=com_docman&task=doc_details&gid=481&Itemid=103

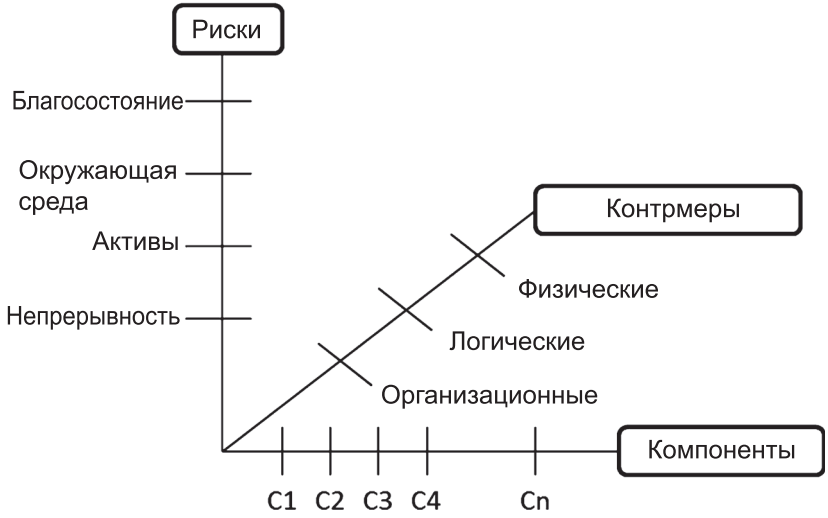


Рис. 1. Три различные точки зрения на критически важную инфраструктуру

3. Системный подход к проектированию

Наиболее важные мероприятия по реализации концепции запланированной безопасности представлены на рис. 2:

Рис. 2. Системный подход к проектированию

3.1. Системный Анализ

Включает в себя следующие этапы:

- выявление функционала критически важной инфраструктуры;
- выявление значимости кибер- и физических компонентов (базы данных, каналы связи и передачи данных, технологические узлы и т.п.) в реализации этого функционала;
- анализ внутренних и внешних интерфейсов, соединяющих компоненты критически важной инфраструктуры между собой и с внешним миром.

Аналитический аппарат должен полностью охватывать всю модель с обратной связью, состоящую из системных моделей как

физической, так и ИКТ инфраструктуры. Методология системного проектирования, разработанная INCOSE (Международный Совет по системному проектированию), является ценным инструментом для проведения системного анализа[4].

3.2. Анализ рисков

Включает в себя следующие этапы:

- выявление потенциальных угроз, которые могут оказать влияние на критически важную инфраструктуру;
- анализ уязвимостей системы/компонентов, которые могут быть использованы определенными злоумышленниками для нанесения ущерба критически важной инфраструктуре;
- выработка метода оценки рисков безопасности с учетом архитектуры и угроз, и его реализация с использованием программных инструментов и алгоритмов.

Результаты этого этапа являются типичными для любого анализа рисков[5]: уязвимости, ущерб (потеря целостности компонента или нарушение функциональности вследствие возникновения причины), причина (т.е. событие, причиняющее ущерб), следствие (т.е. эффект ущерба), угроза и оказанное влияние.

3.3. Анализ безопасности

Включает в себя следующие этапы:

- формирование списка задач по защите, который может быть переведен в формальную семантику с четкими зависимостями и производными из задач. Также формируется список управляющих воздействий и контрмер, используемых для решения задач защиты, соответствующих данному сценарию или конфигурации, и в которых принятие решения может быть частично автоматизировано для определения необходимых и достаточных условий. Эти задачи защиты и механизмы обеспечения безопасности (так как они должны быть реконфигурируемы в условиях атаки или иной деградации) также поддерживают устойчивость ИКТ-систем к пока еще неизвестным типам атак, в том числе частично успешным;
- определение и внедрение с помощью программных инструментов алгоритмов, обеспечивающих проверку предлагаемых контрмер на этапе проектирования. Важно отметить, что анализ

---

[4] INCOSE Systems Engineering Handbook v. 3.2.2, INCOSE-TP-2003-002-03.2.2, October 2011

[5] For instance: Kjølle, G.H. et al. 2012. "Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies." Reliability Engineering and System Safety (2012)

безопасности включает в себя начальный этап проектирования, на котором задаются общие цели (задачи защиты), которые также должны соответствовать условиям эксплуатации. Однако эффективность механизма или фактическая реализация действий по защите и снижению ущерба должны определяться динамически. Это делается для того, чтобы в случае неизбежного изменения конфигурации или в результате нападения, поставленные задачи по защите еще могли бы быть выполнены, или, в случае, если это невозможно, была бы обеспечена соответствующая приоритизация.

3.4. Реализация контрмер

Включает в себя следующие основные этапы:

- стандарты — определение стандартов, необходимых для соответствия необходимым конструктивным параметрам, выявленным на предыдущих этапах;
- определение компонентов системы — четко определить элементы системы, находящиеся под контролем проектной команды и/или организации, и ожидаемые взаимодействия с внешними системами, не находящимися под таким контролем;
- внешние интерфейсы — функциональные и проектировочные интерфейсы взаимодействия с системами и/или персоналом внешним по отношению к процессу разработки;
- функции системы — определение функций системы. Эти функции не должны зависеть от реализации;
- среда (среды) использования — для каждого предусмотренного сценария функционирования системы выявить все факторы окружающей среды (природные и искусственные), которые могут повлиять на производительность системы, оказать влияние на комфорт и безопасность персонала, или вызвать человеческую ошибку;
- технологические требования жизненного цикла — условия и конструктивные особенности, которые обеспечивают эффективность и рентабельность функций жизненного цикла (например, производство, внедрение, развитие, эксплуатация, техническое обслуживание, реинжиниринг/обновление и утилизация);
- особенности проектирования — в том числе интеграция потребностей человека и систем, требования безопасности системы, и потенциальное воздействие на окружающую среду;
- проектные ограничения — в том числе физические ограничения, ограничения на рабочую силу, персонал и иные ресурсы, накладываемые на эксплуатацию системы и взаимодействующих внешних систем.

3.5. Выбор технологий

Специальная публикация Национального института стандартов и технологий США (NIST) 800-36 «Руководство по выбору средств обеспечения безопасности в сфере информационных технологий»[6] охватывает ряд ИТ-средств обеспечения безопасности, предлагаемых к использованию в качестве оперативных или технических средств контроля безопасности. В руководстве рассмотрены следующие вопросы:

- Проводилось ли определение требований безопасности и их сравнение со спецификациями продукции?
- Соответствует ли средство обеспечения безопасности требованиям физической безопасности и иным требованиям политики безопасности?
- Были ли учтены известные уязвимости средства обеспечения безопасности после их рассмотрения?
- Рассматривалась ли политика или позиция поставщика в отношении перепроверки средств обеспечения безопасности после появления их новых версий?
- Каков опыт реагирования поставщика на изъяны безопасности в его продукции?

4. На пути к культуре кибербезопасности

Культура безопасности включает в себя восприятие, культурную среду, скрытое знание и опыт, находящийся за пределами научной и технологической сферы. В целом культура безопасности является частью организации безопасности. Безусловно, в основе мер безопасности заложен ключевой элемент, связанный с доверием и надежностью организации. Культура безопасности является последним звеном цепи, включающей в себя (в данном порядке) «культуру реагирования, культуру профилактики, культуру управления и саму культуру безопасности». Таким образом, единственной эффективной мерой может быть обучение нового поколения ИКТ-специалистов персональной этике.

5. Выводы

Ввиду того, что сложные инфраструктуры меняют своё местоположение, перемещаются по сетям и устройствам, возрастает потребность в защите конфиденциальной информации и критически важных активов без ущерба для мобильности рабочей силы

[6] http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf

или производительности. Учитывая скорость и сложность современных атак и тяжелые последствия нарушения безопасности, решение этих проблем становится всё более сложной задачей для организаций любых размеров. Сейчас стало ясно, что старые модели безопасности больше не отвечают современным вызовам, возникшим в результате повсеместного использования Интернета в каждой сложной инфраструктуре. Старые решения безопасности вытесняются защитой ключевых активов и функций путем обеспечения необходимого уровня защиты для каждой отдельной ситуации и подсистемы.

Sandro Bologna, Maurizio Martellini
Insubria Center on International Security (Italy)

Claudio Calisti
ASTER-TE

ICT Systems for Complex Infrastructures: from Security Technologies to Security Solutions

Introduction

Recent examples of vulnerabilities make evidence that security model of 10 to 15 years ago is no longer adequate to meet contemporary challenges derived from the universal use of Internet in every ICT system. The older model is out-moded and does not scale in the face of today's threats to ICT systems. Perimeter-based security has evolved to a highly distributed model as employees, partners and customers conduct business remotely across the Internet. The security industry has responded with new and enhanced products to meet each new threat appearing on the scenario. All of these tools add some temporary value to overall enterprise security, but they are, in effect, only case by case security solutions facing the single threats. They are not derived from a risk-based, enterprise-wide security program, and the overall effort tends to be fragmented. In many cases, organizations must deal with incomplete data because a given security tool may not recognize a threat or risk for what it is without correlation from other data sources. Diverse security technologies have been developed in response to the evolving threat landscape, what is missing is a methodology that supports the analysis of the security context and only consequently the design of the appropriate solution. An activity that appears innocuous to one part of an infrastructure may be revealed as a threat when it is correlated with the all rest of the infrastructure.

1. Security by Design

As defined by the US Department of State[1]: "Security-by-Design" is a concept that incorporates security in all phases and aspects of facility design, construction, and operations. Security is viewed from a life-cycle management perspective, ensuring that the facility is designed, constructed and maintained in a manner to ensure efficient and effec-

[1] http://www.state.gov/t/isn/rls/fs/186672.htm

tive security operations. Early in the facility design phase, the design is tested against a spectrum of threats through vulnerability assessment and the use of modeling and simulations tools. The design is modified in response to any issues identified and the subsequent changes to the design are evaluated in the same manner, along the life span of the system.

According to SANDIA National Laboratories, the overarching objective of Security-by-Design is to allow mission achievement while security exceeds threat capability[2]. So, security analysis has to be done early in the system design phase, and it has to ensure the appropriate security level during the entire mission achievement, i.e. for the whole system lifetime. The security of the Critical Infrastructure (CI) and that of the ICT system are not mechanically composable. An ICT system can be considered fully secure when stand-alone and where all components and their supply chain meet stringent requirements, while presenting vulnerabilities when integrated in a real operational environment (integration with other components of the overall socio-technical systems, i.e., other ICT systems and networks, human operators, procedures and work practices). When dealing with Critical Infrastructures protection, it is not possible to ensure ICT systems security without taking in detailed account their operational environment, from a technical, architectural and operational perspective. This is also due to the fact that, although Critical Infrastructures control and managing systems are actually ICT systems (they include telecommunications, computers, enterprise software, middleware, storage, display systems, etc.), they have in addition precise real-time and continuity constraints that prevent the use of many of the common ICT countermeasures (e.g. the use of firewall and antivirus, as well as of software update).

While the protection of Critical Infrastructures started dominantly by utilities, the methods for developing secure by design paradigms is still less elaborated. To be effective it has to address the complex interdependencies and interactions originating in a mix of physical and ICT infrastructures, together with operational procedures and human operators. All together they form a system subject of high-level of security requirements. The evolution and changes in the requirements, workloads and other environmental factors necessitate a complex closed loop assessment of the designs and their operation. Moreover; changing key performance indicators like a differently weighted risk, security, throughput, etc., under different conditions necessitate

[2] SANDIA REPORT, Security-by-Design Handbook, SAND2013-0038, January 2013, Albuquerque (US). http://prod.sandia.gov/techlib/access-control.cgi/2013/130038.pdf

at least a set of pre-validated operation scenarios. Such a multi-aspect analysis for existing infrastructures is a core element for the efficient functioning of infrastructures.

The same CI can be observed from different viewpoints[3]. These viewpoints can be considered as "Dimensions" in a 3D space: the Component Dimension, the Countermeasure Dimension, and the Risk Dimension (Figure 1).

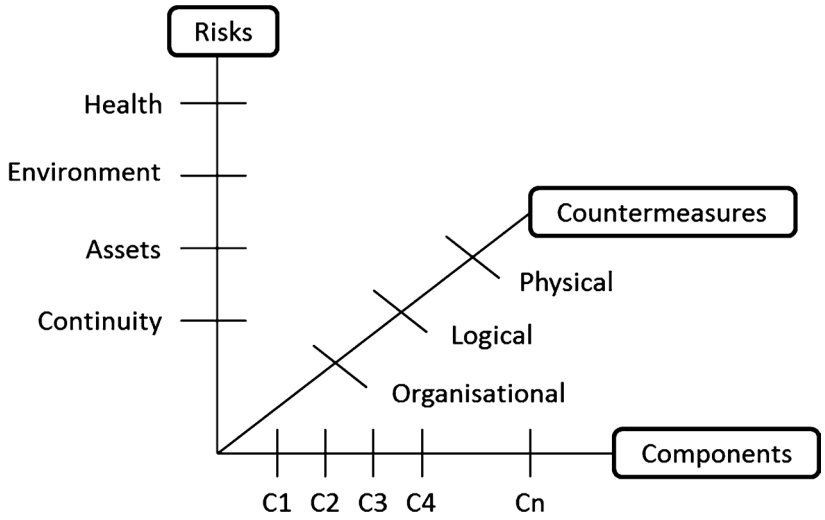


Figure 1. Three different viewpoints of the CI

Each point of the space in Figure 1 represents a countermeasure applied to a system component in order to thwart a specific risk. The Component Dimension entails the decomposition of the CI in sub-elements, which can be either physical or logical. It is therefore possible to define CI Physical and Logical Architectures.

1. System Engineering Approach

Most important activities to implement the concept of Security — by — Design are represented in Figure 2.

1.1. System Analysis

Consists of the following steps:

[3] AIIC Piano di Sicurerzza dell'Operatore: Proposta di line guida operative (in Italian) http://www.infrastrutturecritiche.it/aiic/index.php?option=com_docman&task=doc_details&gid=481&Itemid=103

Figure 2. System Engineering Approach

- The identification of the functionalities implemented by the Critical Infrastructure.
- The identification of the role played by the cyber and physical components (databases, data communication links, process units, etc.) in the implementation of those features.
- The analysis of internal and external interfaces that connect the CI components among them and with the outside world .

The analysis framework has to manage the entire closed loop model composed of both the physical and the ICT infrastructure system models. The Systems Engineering Methodology as defined by INCOSE is a valuable tool to conduct System Analysis[4].

1.2. Risk Analysis

Consists of the following steps:

- The identification of the potential threats that may affect the Critical Infrastructure.
- The analysis of the system/components vulnerabilities that can be exploited by identified threats in order to cause damages to the Critical Infrastructure.
- Definition of the method to evaluate security risks given the architecture and the threats, and implementation via software tools of algorithms.

The outputs of this phase are those typical of any risk analysis[5]: Vulnerability, Damage (Component or Functionality integrity loss due to the occurrence of a Cause), Cause (i.e. the damaging event), Consequence (i.e. the damaging effect), Threat, and Impact.

1.3. Security Analysis

Consists of the following steps:

- Modeling of a set of protection goals which can be translated in formal semantics with clear dependencies and derivations among protection goals. Similarly, a set of controls and countermeasures is to be defined, which are to be employed in support of the protection goals relevant for a given scenario or configuration and where reasoning may

[4] INCOSE Systems Engineering Handbook v. 3.2.2, INCOSE-TP-2003-002-03.2.2, October 2011

[5] For instance: Kjølle, G.H. et al. 2012. "Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies." Reliability Engineering and System Safety (2012)

be partly automated to determine necessary and sufficient conditions. These protection goals and mechanisms for security and — as they are intended to be reconfigurable also in the presence of attacks or other degradation — also serve the resilience of the ICT systems against yet-unknown types of attacks, including partially successful ones.

- Definition and implementation via software tools of algorithms supporting the validation of the proposed countermeasures at the design stage. It is worth noting that this security analysis consists of an initial design stage in which the overall objectives (protection goals) are specified, which must also be matched against operational requirements, but that the strengths of mechanism or actual implementation of protective and mitigating operations should be determined dynamically. This is to ensure that in the inevitable event of configuration changes or as a result from attacks, protection goals can still be satisfied, or where it is not possible to satisfy all or the same level, to have appropriate prioritisation in place.

1.4. Implementation of countermeasures

Consists of the following main tasks:

- Selected standards — Identify standards required to meet design requirements constraints derived from the previous activities.
- Identify system components — Clearly identify system elements under design control of the project team and/or organization and expected interactions with systems external to that control boundary.
- External interfaces — Functional and design interfaces to interacting systems, and/or humans external to the system under development.
- System Functions — Define the functions that the System is to perform. These functions should be kept implementation independent.
- Utilization environment(s) — Identify all environmental factors (natural or induced) that may affect System performance, impact human comfort or safety, or cause human error for each of the operational scenarios envisioned for System use.
- Life-cycle process requirements — Conditions or design factors that facilitate and foster efficient and cost-effective life-cycle functions (e.g., Production, Deployment, Transition, Operation, Maintenance, Reengineering/Upgrade, and Disposal).
- Design considerations — Including human systems integration, system security requirements, and potential environmental impact.
- Design constraints — Including physical limitations, manpower, personnel, and other resource constraints on operation of the System, and interacting systems external to the system boundary.

1.5. Technology Selection

NIST special publication 800-36 "Guide to Selecting Information technology Security Products"[6] covers the selection of IT security products to be used as operational or technical security controls. The guideline address questions like:

- Have security requirements been identified and compared against product specifications?
- Is the security product consistent with physical security and other policy requirements?
- Have known product vulnerabilities been addressed by reviewing the relevant vulnerabilities of a product?
- Has the vendor's policy or stance on re-validation of products when new releases of the product are issued been considered?
- What is the vendor's "track-record" in responding to security flaws in its products?

2. Toward a cyber security culture

Security culture involves perception, culture background, latent knowledge and experience beyond the scientific and technological assets. In general, security culture is a branch of security organization. Indeed, one of the key element is linked with trust and reliability of the organization underpinning the security measures. Security culture is the final step of a chain involving (in order) "responsive culture, preventive culture, management culture, and security culture itself". Therefore, training education in personal ethic for the next generation ICT specialist could be the only effective measure.

3. Conclusions

As complex infrastructures move across locations, networks and devices, there is an increasing need to protect sensitive information and critical assets without having to compromise workforce mobility, or productivity. Given the speed and sophistication of today's security attacks and the severe consequences of a security breach, addressing these challenges is an increasingly complex task for organizations of all sizes. It is now clear that past security models are no longer adequate to meet contemporary challenges derived from the universal use of Internet in every complex infrastructure. Security solutions give the way to meet key assets and functions protection by ensuring the right level of protection for every individual situation and subsystems.

[6] http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf

П.В.Сундеев
ОАО «Мобильные ТелеСистемы»

Перспективы применения Big Data для обеспечения безопасности критических информационных систем

Существует класс информационных систем, обеспечение безопасности которых является одним из основных требований. К ним можно отнести, например, системы управления опасными технологическими производствами, транспортом, объектами управления инфраструктурой и другие. Такие информационные системы называют критическими. Безопасность критических систем во многом зависит от безопасности сетей связи, составляющих основу критической информационной инфраструктуры страны или компании, имеющей критическую систему. На разных этапах процесса обеспечения безопасности критической информационной инфраструктуры или информационной системы необходимо иметь достоверную оценку безопасности информационной архитектуры.

Основные этапы процесса обеспечения безопасности информации, реализация которых требует проведения оценки:

- оценка рисков нарушения безопасности информации;
- анализ информационных потоков и архитектуры;
- анализ модели угроз и нарушителя безопасности информации;
- разработка политики информационной безопасности;
- построение системы защиты информации;
- оценка эффективности системы защиты информации;
- управление процессами защиты информации и инцидентами;
- контроль обеспечения безопасности информации.

Для получения достоверной оценки безопасности сложной информационной системы необходимо провести классификацию и анализ разнообразных физических и логических элементов и связей между ними с учетом динамики изменения состояний, что предполагает использование различных методов моделирования, а также редукции графа состояний для упрощения модели в целях обеспечения разрешимости задачи. Однако любая модель является не точной. При увеличении сложности системы, типов и количества анализируемых объектов точность модели снижается. Для критических информационных систем такая ситуация

не приемлема, поскольку возникает риск реализации инцидентов информационной безопасности с существенным ущербом.

Сочетание методов моделирования с технологиями Big Data дает возможность повышения достоверности результатов динамического моделирования состояний сложных информационных систем при решении задач обеспечения безопасности информации.

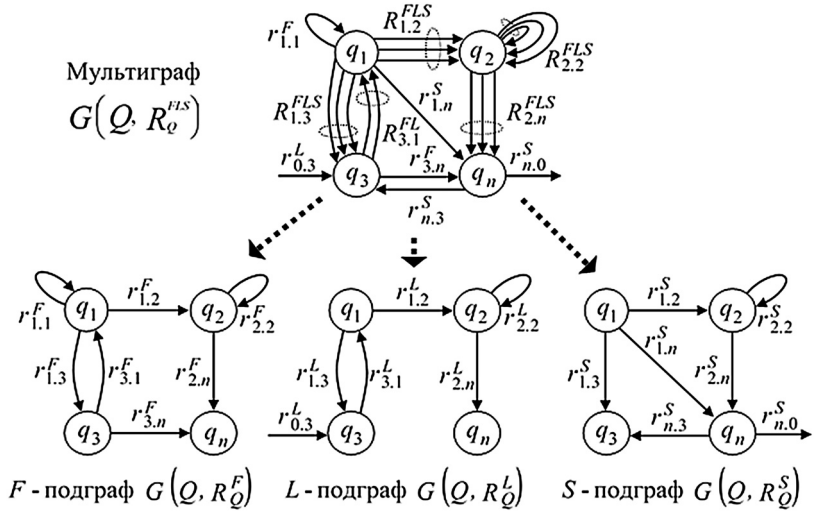
Рассмотрим возможность применения технологии Big Data для построения модели информационной системы и оценки ее соответствия политике безопасности на примере использования модульно-кластерной сети (МКС).

В МКС архитектура критической информационной системы представляется в виде FLS-мультиграфа, вершинами которого являются физические и виртуальные (логические) модули, дугами — информационные отношения между модулями. Типизация модулей проводится на основе анализа их кластерных свойств. Каждое свойство модуля — это интерфейс, определяющий возможность модуля по взаимодействию с другими модулями, имеющими аналогичный (парный) интерфейс. Интерфейсы распределяются по иерархическим уровням информационного взаимодействия: F-физическому, L-синтаксическому и S-семантическому. Набор FLS-интерфейсов модуля определяет его способность к реализации информационных примитивов по обработке информации (передаче, хранению, копированию, изменению и т.п.).

На рисунке представлен упрощенный сегмент мультиграфа состояний модульно-кластерной сети и его декомпозиция на остовные FLS-подграфы.

Если модули имеют однотипные интерфейсы на трех уровнях, то срабатывает переход системы в новое состояние, при котором создаются новые или удаляются существующие модули (вершины графа) и интерфейсы (дуги графа). Наличие уровней взаимодействия модулей позволяет моделировать динамику процесса обработки информации, формализовать политику безопасности и учесть влияние на информационный процесс средств защиты информации. Например, учесть в модели влияние на процесс средств разграничения физического доступа к оборудованию, разграничение на уровне синтаксического доступа к информации криптографическими средствами, семантического доступа средствами разграничения полномочий пользователей и программ. Моделирование смены состояний позволяет найти все возможные траектории информационного процесса. Сравнение декларируемой политики безопасности со всеми состояниями

системы позволяет определить опасные траектории процесса, при которых возможен несанкционированный доступ к объектам защиты. Для обеспечения практической применимости метода к сложным системам граф состояний редуцируется за счет типизации модулей и их интерфейсов, что выводит задачу анализа из класса NP-полных задач. При этом снижается точность модели и достоверность результатов анализа.



Эффективные решения часто находятся в сочетании различных методов. Некоторые направления применения технологии Big Data для решения задач обеспечения безопасности информации уже имеют практическое применение, другие находятся на стадии разработки методологии применения или реализации.

Применение технологии Big Data является перспективным направлением для улучшения результатов моделирования и оценки ИБ в сочетании с методами построения и анализа модульно-кластерной сети, что позволит повысить полноту модели информационной системы, достоверность и применимость результатов анализа за счет:

- сокращения времени построения модульно-кластерной модели КИС (ускорение процедур идентификации и типизации модулей и их интерфейсов);
- представления в модели большего числа и типов элементов и связей, которые редуцируются в стандартных условиях;

- обеспечения мониторинга состояний, управления инцидентами и принятия решений по информационной безопасности в онлайн режиме (ускорение процедур поиска состояний, идентификации аномалий событий безопасности, обеспечение полноты базы знаний для формирования вариантов решений и др.);
- визуализации графа состояний системы с указанием мест нарушения политики безопасности и т.п.

Кроме методических существуют правовые аспекты использования Big Data для решения задач информационной безопасности. Во многих приложениях технологии Big Data используются для анализа персональных данных, в том числе при трансграничной обработке, что может входить в противоречие с национальным законодательством.

В целях обеспечения правовой легитимности целесообразно разработать и принять международный стандарт по обеспечению информационной безопасности Big Data, в котором определить основные принципы их использования, трансграничной передачи, обеспечения прав физических лиц и применения мер защиты. Такой международный стандарт может быть принят, например, Международным союзом электросвязи, в котором функционирует 17-й комитет по безопасности.

Основные принципы обеспечения безопасности персональных данных при использовании технологии Big Data в соответствии с Мавританской резолюцией:

- Открытость в информации о составе собираемых сведений, их обработке, целях использования и передачи третьим лицам.
- Определение цели сбора информации непосредственно во время ее сбора и ограничение использования данных исключительно установленной целью.
- Получение согласия на использование данных.
- Сбор и хранение только того объема данных, который необходим для реализации намеченных законных целей.
- Предоставление персонального доступа лицам к тем данным, которые были собраны о них, обеспечение информацией об источниках данных и любых алгоритмах, используемых для дальнейшего развития их профиля.
- Предоставление лицам возможности исправления и управления своей информацией.
- Проведение анализа того, как сбор информации влияет на неприкосновенность частной жизни пользователя.
- Анонимизация (обезличивание) данных.
- Ограничение и контроль доступа к персональным данным.

- Проведение регулярного анализа для подтверждения того, что результаты профилирования «надежны, справедливы и этичны, а также отвечают той цели, для достижения которой и используются профили».

Выводы:

1. Применение технологии Big Data в целях решения задач обеспечения безопасности информации в критических информационных системах, в том числе, операторами связи, является перспективным направлением повышения уровня защиты информации. В частности, технология позволяет повысить достоверность оценки безопасности информации в критических приложениях.

2. Целесообразно стандартизировать вопросы безопасного применения технологии Big Data для использования в области обеспечения ИБ на международном уровне, гармонизировать законодательство под новые реалии информационного общества.

P.V.Sundeev
Mobile TeleSystems

Prospects of application of Big Data for security-critical information systems

There is a class of information systems, for which security is one of the basic requirements. It includes, for example, control systems of: hazardous industrial processes, transportation, facilities management, and of other infrastructure. Such information systems are called critical. Security of critical systems largely depends on security of communication networks that form the foundation of critical information infrastructure of a country or a company with a critical system. At different stages of the process of ensuring security of critical information infrastructure or information system it is necessary to have a reliable assessment of information architecture security.

The principal stages of information security process, the implementation of which requires an assessment:

- assessment of information security risks;
- analysis of information flows and architecture;
- analysis of threat model and violator's model;
- development of information security policy;
- development of an information security system;
- assessment of effectiveness of information security system;
- management of information security processes and incidents;
- control of information security.

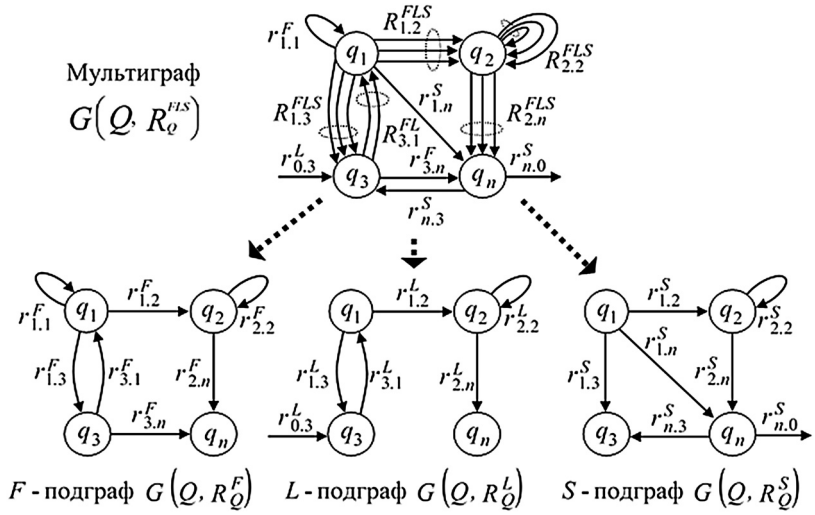
Reliable assessment of a complex information security system requires classification and analysis of various physical and logical components and connections between them, with consideration for dynamics of state changes, which implies the use of different modeling approaches and state graph reduction to simplify the model in order to ensure the solvability of the problem. However, no model is fully accurate. Increase in complexity of the system, types and amount of analyzed objects reduces the model's accuracy. This situation is not acceptable for critical information systems, since it brings about the risk of information security incidents with significant damage.

The combination of modeling techniques with Big Data technology makes it possible to increase reliability of the results of dynamic state modeling of complex information systems for solving problems of information security.

Further on we will investigate the possibility of applying Big Data technology to construction of an information system model and assessment of its compliance with security policy on the example of modular cluster network (MCN).

The architecture of critical information systems is presented in MCN in the form of FLS-multigraph, whose vertices are the physical and virtual (logical) modules, and arcs are information relations between the modules. Type assignment of the modules is based on analysis of their cluster properties. Each property of a module is an interface, which determines the possibility of its interaction with the other modules that have the same (matching) interface. Interfaces are distributed through the hierarchies of informational interaction: F-physical, L-syntactic and S-semantic. Module's set of FLS-interfaces determines its ability to implement information primitives of information processing (transmission, storage, copying, modification, etc.).

The diagram shows a simplified segment of a modular cluster network states multigraph and its decomposition into spanning FLS- subgraphs.



If modules have the same type of interface on three levels, it triggers a transition of a system to a new state in which the new modules (vertex) and interfaces (arcs of the graph) are created or existing ones are deleted. Presence of module interaction levels allows one to simulate the dynamics of information processing, formalize the security policy

and take into account the impact of information security tools on the information process. For example, to take into account an impact of physical access control, information access control by cryptographic means on syntax level, control of semantic access by means of division of access rights of users and programs. State change simulation allows you to find all the possible trajectories of the information process. Comparison of the declared security policy with all the states of the system makes it possible to determine dangerous paths of the process, which are susceptible to unauthorized access to protected objects. To ensure the practical applicability of the method to complex systems, the state graph is reduced by type assignment of modules and their interfaces. This takes the task out of the category of NP-complete problems. This also reduces the accuracy of the model and the reliability of the analysis results.

Efficient solutions are often found in a combination of different methods. Some areas of Big Data application to issues of information security have already found practical use, while others are on a stage of development or implementation of their methodology.

Application of Big Data technology in conjunction with the methods of design and analysis of module-cluster network is a promising avenue for improving the results of modeling and evaluation of information security. It will enhance the completeness of information system model, accuracy and applicability of the analysis results by:

- reduction of time needed for construction of module-cluster model of critical information systems (the acceleration of identification and type assignment procedures for modules and their interfaces);
- representation of larger amounts and types of elements and connections in the model, which are reduced under standard conditions;
- ensuring the monitoring of states, incident management and decision-making on information security in online mode (acceleration of search procedures for states, identification of security events anomalies, ensuring knowledge base completeness for decision-making, etc.);
- visualization of a system states graph with indications of security policy violations etc.

In addition to methodical, there are legal aspects of Big Data use for solution of information security issues. Big Data technologies are used in many applications for the analysis of personal data, also with cross-border information processing, which may contravene national legislation.

In order to ensure the legal validity, it is viable to develop and adopt an international standard for information security of Big Data, which would define the basic principles of its use, cross-border transmission,

protection of rights of individuals and use of security measures. The corresponding international standard can be adopted, for example, by International Telecommunication Union, where there is the 17th Committee on security.

Basic principles of personal data security when using Big Data technologies in accordance with the Moresco resolution:

- Openness of information on composition, processing, purposes of use and transfer to third parties of collected data;
- The purpose of information collection is determined during the actual collection and the use of data is restricted by a determined purpose;
- Receive consent to data usage;
- Collection and storage of the right amount of data required for implementation of the determined legitimate purposes;
- Granting personal access for individuals to data collected about them, provision of information about the sources of the data and all the algorithms used for further development of their profile;
- Provide an option for individuals to correct and manage their information;
- Analysis of how collection of information affects user privacy;
- Anonymization (depersonalization) of data;
- Restriction and control of access to personal data;
- Regular analysis to confirm that profiling results «are reliable, fair and ethical, and serve the purpose they are used for».

Conclusions:

1. The use of Big Data technology to address the problems of information security in critical information systems, in particular by telecom operators, is a promising way to increase the level of data protection. In particular, the technology can improve the assessment accuracy of information security of critical applications.

2. For application in information security at international level it is advisable to standardize the aspects of safe use of Big Data technologies, to harmonize the legislation with regard to new realities of information society.

А.А.Сальников, П.Л.Пилюгин

Институт проблем информационной безопасности
МГУ имени М.В.Ломоносова

Безопасность, стабильность и отказоустойчивость инфраструктуры глобального Интернета

Определения понятий безопасность, стабильность и отказоустойчивость

Предметом настоящей статьи являются вопросы безопасности, стабильности и отказоустойчивости глобальной инфраструктуры сети Интернет. При этом область исследования ограничена только теми вопросами, которые входят в мандат ICANN. Поэтому, прежде всего, приведем определения понятий «безопасность», «стабильность» и «отказоустойчивость» в том виде, как их определяет сама корпорация ICANN (см. [1]):

Безопасность — способность предотвращать и ограждать от неправильного использования уникальных идентификаторов сети Интернет.

Стабильность — возможность гарантировать, что система функционирует в соответствии со своим регламентом, а также способность обеспечить уверенность пользователей системы уникальных идентификаторов в том, что это именно так.

Отказоустойчивость — способность системы уникальных идентификаторов эффективно противостоять/выдерживать/переживать злонамеренные атаки и другие разрушающие события без ущерба и без прекращения выполняемых системой функций.

Приведенные выше понятия имеют фундаментальное значение, но определения этих понятий требуют уточнений для соответствия современному их значению и для гармонизации с существующими международными и национальными нормативными документами и стандартами, использующими эти понятия.

Основными причинами необходимости уточнения этих понятий являются:

1. Неоднозначность толкования этих понятий. Во многих работах «стабильность» и «отказоустойчивость» рассматриваются как составные части общего понятия «безопасность» и, вследствие этого, явно или неявно входят в это общее определение. Более того, понятия «стабильность» и «отказоустойчивость» часто соотносятся с понятием «надежность», а само толкование

термина «безопасность», через «неправильное использование» допускает очень широкую интерпретацию.

2. Проблемы лингвистического характера. При переводе с/на английский язык часто теряются или возникают новые, дополнительные коннотации. Базовое понятие «безопасность» в русском языке (и, что в данном случае даже более важно — в российских документах) прежде всего, означает «состояние защищенности», в то время как клише английского перевода «security», кроме этого, подразумевает и совокупность средств, обеспечивающих это состояние защищенности. Попытка использовать для перевода английское слово «safety» также не слишком удачно, т.к. оно несет оттенок «*внутреннее ощущение* защищенности», что, вообще говоря, отсутствует в русском эквиваленте (см. [2]). Непонимание этих нюансов часто приводит к долгим (и бессмысленным!) спорам при обсуждении конкретных вопросов на международных площадках.

3. Область применения понятий. Приведенные выше определения ограничены понятиями безопасности (стабильности и отказоустойчивости) в части функций, исполняемых ICANN (может быть, даже более точно — IANA), а именно в части системы распределения уникальных идентификаторов, номеров и параметров. В то же время к критически важной инфраструктуре глобального Интернета относятся также а) инфраструктура магистральных сетей передачи данных (оптических, спутниковых и др.) и б) сервисные платформы, обеспечивающие пользователям предоставление базовых услуг. Для них также должны быть определены соответствующие им понятия «безопасности» и «устойчивости», но в настоящей статье эти вопросы не рассматриваются.

4. Условия применимости понятий. Кроме приведенных выше замечаний в отношении определения этих понятий необходимо учитывать условия, в которых эти понятия сохраняют свои значение. Инфраструктура сети Интернет сохраняет свою работоспособность в условиях «нормальной» работы сети. Между тем в ряде исследований (см., например, материалы Таллиннского Центра кибербезопасности НАТО [10],[11]) рассматриваются условия функционирования сети как в случае «нормальных», так и в случае «экстремальных» условий ее функционирования, что также требует соответствующего уточнения значения этих фундаментальных понятий.

5. Соответствие международным и национальным нормативным документам. Существует целый пул международных (ISO), национальных (NIST, ГОСТ и пр.) и ведомственных стандартов в

области безопасности и надежности, относящихся не только к информационным системам (см. обзор [8]), в которых зафиксирована терминология, соответствующая этой предметной области. Помимо вынесенных в заголовок терминов «стабильность» (stability) и «отказоустойчивость» (resiliency), используются близкие понятия «надежность» (dependability), «безотказность» (reliability), «живучесть», «ремонтопригодность» и пр. Отдельный блок стандартов относится к вопросам управления рисками (см. ГОСТ Р 51897-2002 «Менеджмент риска. Термины и определения»; ISO/МЭК 73:2002 «Управление риском. Словарь. Руководящие указания по использованию в стандартах»). Терминология, зафиксированная в этих стандартах, также имеет серьезные пересечения с понятиями, зафиксированными в руководящих документах ICANN[1].

Таксономия понятий безопасность, стабильность и отказоустойчивость

Все вышесказанное относится лишь к отдельным элементам глобальной информационной системы Интернет. Понятия «безопасность», «стабильность» и «отказоустойчивость» как системы уникальных идентификаторов, так и сервисных платформ и инфраструктуры магистральных сетей входят в общее понятие «информационной (кибер) безопасности». Таксономия понятий «информационная безопасность», «кибербезопасность», «безопасность информации», «безопасность информационно-коммуникационных технологий» и т.д. является предметом обсуждения многих международных конференций, как академических, так и политических (см. например, [9]). В силу самых

---

[1] Для иллюстрации приведем несколько формулировок Национального института стандартов США NIST (см. [3]):

Безопасность — состояние, являющееся результатом внедрения и поддержания работоспособности защитных мер, которые позволяют системе выполнять свои функции, несмотря на риски реализации угроз ее работоспособности. Защитные меры могут включать совокупность мер сдерживания, избегания, предотвращения, отслеживания, восстановления и исправления. В совокупности эти меры являются частью системы управления рисками.

Отказоустойчивость — способность быстро адаптироваться и восстанавливаться после любых известных или неизвестных изменений в окружающей систему обстановке путем комплексного применения системы управления рисками и непрерывного планирования.

Речь идет о способности (а) продолжать функционировать и выполнять ключевые функции во враждебных условиях и воздействиях даже при частичном разрушении самой системы и (б) восстанавливаться до состояния, позволяющего выполнять предписанные функции за время, определяемое миссией системы.

разных причин (включая, конечно, и политические) до консенсуса в этом вопросе еще очень далеко. Приведем компромиссную формулировка понятия «кибербезопасность», выработанную в ходе выполнения совместного проекта Института проблем информационной безопасности (ИПИБ) МГУ и Института Восток-Запад (EWI) США, см. [2]:

Кибербезопасность — свойство киберпространства (киберсистемы) противостоять намеренным и/или ненамеренным угрозам, а также реагировать на них и восстанавливаться после воздействия этих угроз.

Полезно отметить, что в том же проекте ИПИБ МГУ — EWI ([2]) изложено соотношения понятий с приставкой «кибер-» и «инфо-».

В Российской Федерации первоисточником трактовки понятий, связанных с вопросами безопасности, следует считать Закон Российской Федерации «О безопасности» № 2446-I (см. [4]):

Безопасность — состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Определения всех остальных видов безопасности (военно-политической, экономической, экологической и пр.), включая понятие информационной безопасности, строятся на основе этого общего определения путем уточнения, о какой сфере общественных отношений идет речь. Для иллюстрации приведем определение информационной безопасности в том виде, как это сформулировано в ряде международных документов, подписанных Российской Федерацией (см., например, [5]):

Информационная безопасность — состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве.

Отметим два методически важных момента, связанных с последними определениями:

- Содержание понятия «безопасность» раскрывается только (а) в привязке к конкретным интересам пользователей и (б) в отношении конкретных угроз этим интересам.
- Понятие «безопасность» увязано с интересами субъектов — пользователей информационной системой. Такая увязка на уровне базовых определений ведет к определенным методическим проблемам при оценке безопасности сложных (а тем более глобальных) систем. Проблема заключается в том, что у различных пользователей системы могут быть взаимоисключающие, противоречащие

друг другу интересы (без привязки к анализируемой информационной системе). Поэтому при оценке защищенности их интересов в связи с анализируемой системой возникнут противоречия, не связанные с функциями/услугами, выполняемыми системой.

Принципиально важно разделить угрозы на два класса: (1) угрозы, возникающие в силу случайных обстоятельств, непреднамеренных ошибок, перегрузок системы, стихийных бедствий, аппаратных сбоев, аварий и т.п., и (2) угрозы, сознательно планируемые, разрабатываемые и реализуемые одними пользователями системы в отношении других пользователей.

Именно последний тип угроз определяет принципиальную разницу двух понятий: «безопасность» и «надежность». Когда речь идет о безопасности, то предполагается наличие субъекта, порождающего угрозы. В то время, когда говорят о надежности, то наличие такого субъекта либо вообще не предполагается, либо он рассматривается неявно, т.е. источником угрозы являются естественные причины (например, перегрузки, сбои, старение материалов и т.д.), природные явления (ураганы, наводнения и т. п.) или неумышленные ошибки (прежде всего ошибки проектирования или написания кодов). При этом, как правило, стремятся уйти от рассмотрения сценариев и свести обсуждение только к выявлению (абстрактных, не увязанных с их источником) уязвимостей. В этом подходе есть определенная доля лукавства и/или проявление методологической ошибки. А именно, приведем определение понятия «уязвимость» по [3]:

Уязвимость — слабость информационной системы, процедур безопасности системы, процедур внутреннего контроля или их реализации, которые могут быть использованы источником угрозы.

Таким образом, в самом определении появляется этот самый субъект — источник угроз (определение по [3]):

Источник угроз — замысел и метод, имеющие целью *намеренное* использование уязвимости или сложившейся ситуации, а также метод, который может непреднамеренно активировать уязвимость.

По нашему мнению, при оценке безопасности системы в отношении преднамеренных угроз методически точнее использовать хорошо известную в Theory of Computer Science, математической криптологии (см., например, [6]) схему.

1. Описывается сама *Система*, т.е. перечисляют функции и услуги, оказываемые *Системой*. Декларируют, какие при этом качества, свойства функций/услуг должна обеспечить *Система* и какие меры/механизмы безопасности она реализует.

2. Определяются *Участники*: а) Пользователь системы, на кого нападают (*Пользователь-жертва*); б) Пользователь системы, который нападает (*Нападающий*).

3. Формулируют *Цели атаки (угрозы)*, которых хочет достичь *Нападающий* (каким именно интересам *Пользователя-жертвы* он стремится нанести ущерб). В данной трактовке *Цель атаки* — это нарушение какой-либо функции или качества услуги *Системы*, используемой *Пользователем-жертвой*.

4. Определяют, какими *Ресурсами* располагает *Нападающий* для достижения *Цели атаки* — к каким элементам *Системы* он имеет доступ, что он может при этом делать и т.п.

Важно подчеркнуть, что при этом изучается *только качество механизмов и мер безопасности*, реализуемых *Системой*. Мотивы атаки (политические, экономические, религиозные и т.д.) здесь не рассматриваются. Здесь отсутствуют эмоциональные (политические) оценки типа *Пользователь-жертва* — «хороший», а *Нападающий* — «плохой»: в качестве *Пользователя-жертвы* при анализе, вообще говоря, можно рассматривать и «Плохого парня» (Bad Guy), интересы которого (например, сохранение анонимности) стремятся нарушить *Нападающие* — «Хорошие парни», например правоохранительные органы.

Перечисленные выше 4 позиции являются исходными данными для оценки степени/уровня безопасности *Системы*. В ходе анализа рассматривают все возможные (гипотетически вообразимые) способы реализации *Нападающим* данной *Атаки*. Если при этом выясняется, что для достижения своих *Целей* при любом вообразимом способе реализации атаки *Нападающему* требуются ресурсы (финансовые, временные, организационные), превышающие разумные параметры, то *Система* признается безопасной в отношении данной *Атаки*. Для оценки безопасности *Системы* в целом необходимо проделать такой анализ для всех пар (*Пользователь-жертва — Нападающий*) и всех *Атак*. Обратим здесь внимание, что при оценке безопасности системы в целом, вообще говоря, *каждый* пользователь системы должен рассматриваться и как потенциальная жертва, и как потенциальный Нападающий!

Предложения по уточнению понятий безопасность, стабильность и отказоустойчивость в соответствии с мандатом ICANN

Применение описанного выше формального подхода к оценке безопасности глобальной инфраструктуры Интернета, на наш

взгляд, позволит во многом расставить точки над i в международных дискуссиях и при наличии доброй воли (заинтересованности) всех участников политического процесса перевести эти дискуссии в конструктивное русло.

Рассмотрим, к чему приводит применение данной методики в отношении оценки безопасности глобальной инфраструктуры распределения уникальных идентификаторов, номеров и параметров сети Интернет, в соответствии с многоуровневой моделью инфраструктуры Интернета.

1. ***Система*** (глобальная инфраструктура) распределения уникальных идентификаторов, номеров и параметров сети Интернет является, прежде всего, информационной системой. Причем таких информационных систем может быть несколько, так как в соответствии с многоуровневым представлением инфраструктуры для уровня приложений речь идет о системе доменных имен, а для сетевого и транспортного уровней — о номерах автономных систем, IP-адресах и номерах портов. И как всякая информационная система она, вообще говоря, выполняет/предоставляет возможность реализации всего необходимого набора функций по обработке, распространению, хранению, поиску и предоставлению информации.

- В нашем случае под «информацией» понимаются данные об уникальных идентификаторах, номерах и параметрах сети Интернет, а также вся сервисная (вспомогательная) информация, необходимая для выполнения перечисленных выше функций. В определении «безопасности», даваемом в уставе ICANN, понятие «неправильное использование» следует отнести к *каждой* из этих функций.
- Элементы системы включают в себя ICANN (IANA), структуру 13 корневых серверов и их зеркала, включая набор функций, выполняемых VeriSign, пять региональных RIR-ов, национальные и региональные интернет-регистраторы (NIR, LIR), провайдеры и т.д. Описание элементов системы включает в себя:
  - ◊ назначение по обработке того или иного вида информации (доменные имена, номера автономных систем, IP-адреса и номерах портов);
  - ◊ описание технических средств, реализующих функции системы (hardware, firmware, software);
  - ◊ совокупность технических и организационных стандартов, регламентов и процедур;
  - ◊ юрисдикцию, в рамках которой функционируют элементы системы.

3. Пользователи — это все, кто входит в состав «всех заинтересованных лиц» (stakeholders), именно так, как это принято понимать в текущих дискуссиях:

- субъекты международного права: государства, коалиции и союзы государств, негосударственные автономии и т.п.;
- бизнес (национальный, транснациональный и т.п.), в том числе бизнес «вокруг» инфраструктуры сети Интернет;
- субъекты гражданского общества: политические партии, отдельные Церкви, Религии и их течения (причем, возможно, с экстремистскими целями), организационно оформленные общественные движения, неформальные союзы и объединения ученых и инженеров, и пр.;
- неформальные виртуальные группы пользователей Интернет, объединенные совместными интересами (“Anonymous”, игроки виртуальных сетевых игр, участники «клубов по интересам», и пр.)
- в отдельный блок следует выделить формальные и неформальные объединения разработчиков, инженеров, формирующих облик Интернета (ISOC, IETF и т.д.)
- граждане и частные лица (в число которых неизбежно входят и граждане, имеющие преступные намерения).

3. ***Угрозы*** безопасности в отношении информационной системы в «классическом» понимании включают угрозы в отношении «триады» свойств — C.I.A.:

- Confidentiality — конфиденциальность;
- Integrity — целостность;
- Availability — доступность.

В нашем случае может показаться, что первая из угроз — угроза конфиденциальности — не актуальна, по крайней мере, в отношении уникальных идентификаторов, номеров и параметров сети Интернет (так как сложно представить причину, по которой кому-либо потребуется «засекретить» IP-адрес или имя хоста). Однако сервисная информация, используемая в этих системах, может содержать информацию, составляющую коммерческую тайну или персональные данные физических лиц. Поэтому в рассматриваемом случае требуется обеспечить все свойства — конфиденциальность, целостность и доступность.

При этом необходимо учитывать, что во-первых, эти угрозы необходимо соотнести с уровнями модели инфраструктуры Интернета и если на уровне приложений речь идет о безопасности системы доменных и работы всех серверов доменных имен (DNS), то на сетевом и транспортном уровне наиболее актуальны

задачи обеспечения маршрутизации, как в локальных сетях, так и на уровне взаимодействия автономных систем.

И во-вторых, в данном контексте следует обратить внимание еще на один аспект. Большая часть элементов рассматриваемой инфраструктуры являются коммерческими организациями, основной мотив деятельности которых заключается в извлечении прибыли. Поэтому следует иметь в виду угрозы в отношении доступности и целостности в результате «выпадения» из системы (прекращение или ограничение деятельности) отдельных ее частей в силу самых разнообразных внешних (банкротство, решение суда, санкции, революции и т. п.) и внутренних (низкая рентабельность, смена сферы деятельности, политическая или моральная мотивированность и т. п.) причин.

4. ***Ресурсы***, которыми располагает *Нападающий* (а это может быть любой из тех самых stakeholder-ов!) для реализации своих целей (т.е. для нарушения целостности и/или доступности уникальных идентификаторов, номеров и параметров, принадлежащих *Жертве* или к которым обращается *Жертва*), существенным образом определяются тем, кто является этим *Нападающим*. В частности, наибольшими возможностями и наиболее тяжелые последствия могут наступить в результата атак со стороны центральных\узловых элементов системы (провайдеров, регистраторов, регуляторов и т. д.) И именно в этом, по-видимому, заключается наиболее «спорный» и «деликатный» момент. Так, например, сейчас уже очевидно, что не удастся проигнорировать и замолчать недоверие ряда stakeholder-ов к техническим и программным средствам, обеспечивающим выполнение ключевых функций системы. То же самое относится и к криптографическим механизмам, реализуемым компанией VeriSign.

Вообще говоря, каждый из stakeholder-ов формирует самостоятельно модель угроз своей безопасности, исходя из своих приоритетов. Государства и бизнес-структуры, как правило, это делают явно, в форме нормативного документа (общедоступного или «закрытого»); обычные пользователи «имеют в виду», что именно для них может представлять опасность, а многие на эту тему даже не задумываются и «делают как все». Очевидно, что модели угроз различных stakeholder-ов в большинстве будут противоречить друг другу. По-видимому, наиболее прагматичным подходом для разрешения этих противоречий и недопониманий, является применение описанной выше методики и выработка путем переговоров набора недостающих мер «сдержек и противовесов» (check&balance) балансирующих интересы пользователей,

например, недоверие к отдельным техническим элементам системы, можно «сбалансировать» принятием нормативно-правового документа, обязывающего гарантировать безопасность этих элементов и т.п.

Список цитируемых источников

[1] *ICANN's FY 14 Security, Stability and Resiliency Framework*; https://www.icann.org/public-comments/ssr-fy14-2013-03-06-en

[2] *Critical Terminology Foundations 2. Russia-U.S. Bilateral on Cybersecurity policy report 2/2014*; James B.Godwin III, Andrey Kulpin, Karl Frederick Rauscher and Valery Yaschenko (Chief Editors); https://dl.dropboxusercontent.com/u/164629289/terminology2.pdf

[3] *NISTIR 7298 Revision 2 Glossary of Key Information Security Terms*; Richard Kissel, Editor; Computer Security Division Information Technology Laboratory; May 2013; http://dx.doi.org/106028/NIST.IR.7298r2

[4] *Закон Российской Федерации «О безопасности» № 2446-I* (с изменениями от 25 декабря 1992 г., 24 декабря 1993 г., 25 июля 2002 г., 7 марта 2005 г., 25 июля 2006 г., 2 марта 2007 г.); *http://www.scrf.gov.ru/documents/20.html*

[5] Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности; 16 июня 2009 г.

[6] *http://www.cryptography.ru*

[7] Internet Governance and the Domain Name System: Issues for Congress; Lennard G. Kruger Specialist in Science and Technology Policyб November 26, 2014, Congressional Research Service, 7-5700, www.crs.gov R42351

[8] Струков А.В.; Анализ международных и российских стандартов в области надежности, риска и безопасности; http://szma.com/standarts_analysis.pdf

[9] Пятый международный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении информационной безопасности и противодействия терроризму», 25–28 апреля 2011 г., Гармиш-Партенкирхен, Германия

[10] The Tallinn Manual on the International Law Applicable to Cyber Warfare, http://www.cambridge.org/ca/academic/subjects/law/humanitarian-law/tallinn-manual-international-law-applicable-cyber-warfare

[11] NATO Cooperative Cyber Defense Centre of Excellence free e-book entitled «Peacetime Regime for State Activities in Cyberspace», including a chapter on Space Law and Unauthorized Cyber Activities. https://ccdcoe.org/multimedia/peacetime-regime-state-activities-cyberspace.html

A.A.Salnikov, P.L.Pilyugin

Moscow State University
Institute of Information Security Issues

Security, stability and resiliency of the global Internet infrastructure

In this paper we examine the issues of security, stability and resiliency of the global Internet infrastructure. At that the scope of this research is limited only to the issues that are included in the ICANN mandate. Therefore, first of all we will examine «security», «stability» and «resiliency» as they are defined by the ICANN [1]:

Security — the capacity to protect and prevent misuse of Internet unique identifiers.

Stability — the capacity to ensure that the system operates as expected, and that users of the unique identifiers have confidence that the system operates as expected.

Resiliency — the capacity of the unique identifier system to effectively withstand/tolerate/survive malicious attacks and other disruptive events without disruption or cessation of service

The abovementioned concepts are fundamental, but their definitions need rectification to meet their present meaning, and to be harmonized with the existing international and national regulations and standards, which use these concepts.

The main reasons behind the need to rectify these concepts are:

1. The ambiguity of their interpretation. In many articles «stability» and «resiliency» are considered as parts of the overall concept of «security» and, therefore, are explicitly or implicitly included in this general definition. Moreover, the concepts of «stability» and «resilience» are often correlated with the concept of «reliability», and interpretation of «security» by the notion of «misuse» allows for a very broad interpretation.

2. Issues of a linguistic nature. When translating from/into English, additional connotations are often lost or created. The basic concept of «security» in Russian (and more important in this case — in the Russian documents) primarily means «the condition of security», whereas the cliché of the English translation of «security» implies, apart from that, a set of means that ensure this condition of security. Attempts to use in translation the English word «safety» will not be very successful as well, because it carries a connotation of an «inner sense of security»,

which, generally speaking, has no equivalent in Russian [2]. Failure to understand these nuances often leads to long (and useless!) disputes during discussions of specific issues in international venues.

3. Scope of concepts' application. In part of the functions of ICANN (perhaps even more accurately — of IANA), the abovementioned definitions are limited by the notions of security (stability and resiliency), namely with regard to DNS and the distribution system of unique identifiers, numbers and settings. At the same time, the critical infrastructure of the global Internet also includes a) backbone data networks infrastructure (optical, satellite, etc.) and b) service platforms, which provide the users with basic services. These also need a definition of corresponding concepts of «security» and «stability», but these issues are not addressed in this article.

4. Conditions for concepts' application. In addition to the abovementioned comments regarding the definition of these concepts, one must take into account the conditions under which these concepts keep their meaning. Internet infrastructure retains its working capacity under the «normal» working conditions of the network. Meanwhile, a number of studies (see e.g. the materials of Tallinn NATO Cooperative Cyber Defence Centre of Excellence [10], [11]) consider both «normal» and «extreme» conditions of its functioning, and this also requires appropriate rectification to clarify the meaning of these fundamental concepts.

5. Compliance with international and national regulations. There is a number of international (ISO), national (NIST, GOST, etc.) and departmental safety and reliability standards, which pertain not only to information systems [8], and which include formalized terminology associated with this subject. In addition to headline terms «stability» and «resiliency», similar concepts of «dependability», «reliability», «durability», «maintainability», etc. are used. A separate set of standards governs risk management (see GOST R 51897-2002 «Risk management. Terms and definitions»; ISO / IEC 73: 2002 «Risk management. Glossary. Guidance on the use of standards»). The terminology which is formalized in these standards also has major overlap with the concepts enshrined in the ICANN bylaws[1].

---

[1] To illustrate this we provide several definitions of NIST [3]:

Security — A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.

Taxonomy of security, stability and resiliency

All of the above applies only to individual elements of the global information system of the Internet. The concepts of «security», «stability» and «resilience» in unique identifier systems, service platforms and backbone networks infrastructure are all included in the general concept of «information (cyber) security». Taxonomy of «information security», «cybersecurity», «security of information», «security of information and communication technologies», etc. is a topic of discussion on the agenda of many international conferences, both academic and political (see e.g. [9]). Due to various reasons (including, of course, political) consensus on this issue is a long way down the road. Here we'll mention the consensus definition of «cybersecurity», formulated in the course of a joint project of the Institute of Information Security Issues (IISI) of Moscow State University and the EastWest Institute (EWI) [2]:

Cybersecurity is a property of cyber space that is an ability to resist intentional and unintentional threats and respond and recover.

It is useful to note that the same IISI-EWI joint project [2] touches upon the correlation between derived «cyber» and «information» concepts.

The primary source for interpretation of security concepts in the Russian Federation is the Law «On security» № 2446-I. [4]

Security — a condition of protectability of the vital interests of individuals, society and the State from internal and external threats.

The definitions of all the other types of security (politico-military, economic, environmental etc.), including the concept of information security are based on this general definition and clarify it for specific spheres of social relations. By the way of illustration we consider the definition of information security as it is formulated in a number of international documents, signed by the Russian Federation (see, e.g. [5]):

Information security — security of individual, society, state and their interests from threats, destructive and other negative impacts in information space.

It is necessary to take note of two methodically important aspects related to the latter definitions:

Resilience — The ability to quickly adapt and recover from any known or unknown changes to the environment through holistic implementation of risk management, contingency, and continuity planning.

The ability to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs.

- The scope of the concept «security» is articulated only (a) in relation to the specific interests of users and (b) with regard to the specific threats to these interests.
- The concept of «security» is tied in with the interests of the subjects — users of an information system. Such linkage at the level of basic definitions leads to certain methodological problems when assessing the security of complex (let alone global) systems. The problem is that different users of the system can have mutually exclusive, conflicting interests (without reference to the analyzed information system). Therefore, when assessing the security of their interests with reference to the analyzed system there will be contradictions which are not related to the functions/services provided by the system.

It is essential to break the threats down into two classes: (1) threats emanating from accidental circumstances, unintentional errors, system overload, natural disasters, hardware failures, accidents, etc., and (2) threats which are deliberately planned, developed and implemented by some users of the system against the other users.

It is the latter class of threat that determines the fundamental difference between the concepts of «security» and «reliability». When it comes to security, it is assumed that there is a subject that generates threats. When considering reliability, the presence of such a subject is either not expected or is considered implicitly, i.e. the sources of threats are natural causes (such as overloading, failures, aging of materials, etc.), natural phenomena (hurricanes, floods, and so on) or unintentional errors (primarily design flaws or software coding errors). At that, as a rule, there is a tendency to depart from reviewing scenarios and narrow the discussion down just to identification of (abstract, not linked to their source) vulnerabilities. In this approach, there is a certain percentage of deceit and/or manifestation of a methodological error. More specifically, we provide a definition of the concept of «vulnerability» [3]:

Vulnerability — a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Thus, that very subject — the source of the threat — is included in the definition [3]:

Threat source — the intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability.

In our opinion, when assessing the security of the system with regard to deliberate threats it is methodologically more accurate to use

the procedure well-known in the Theory of Computer Science and Mathematical Cryptology (see, e.g., [6]).

1. Description of *the System* itself, i.e. listing of functions and services provided by *the System*. It is declared what qualities, properties of functions/services the System must ensure and what security measures/mechanisms does it implement.

2. Identification of *the Participants*: a) The system user who is a target of the attack *(the Victim user)*; b) The system user, who attacks *(the Attacker)*.

3. Formulation of *Attack objectives (threats)*, which the *Attacker* seeks to achieve (exactly which interests of the *Victim user* he seeks to damage). In this interpretation the *Attack objective* is an impairment of any function or service quality of the *System* used by the *Victim user*.

4. It is determined what *Resources* are available to the *Attacker* to accomplish the *Attack objectives* — which elements of the system he has access to, and given that, what he can do, etc.

It is important to emphasize that the only thing under study here is the *quality of the security mechanisms and measures* implemented by the *System*. Motives for the attack (political, economic, religious, etc.) are not considered. There is no emotional (political) assessment like *the Victim user* — is «good», and *the Attacker* — is «bad»: generally speaking, in the analysis the Bad Guy can be considered a Victim user, whose interests (e.g., anonymity) are being damaged by *the Attackers* — *the Good guys*, such as law enforcement agencies.

The four abovementioned items are the initial data for assessing the degree/level of security of the *System*. The analysis considers all possible (hypothetically imaginable) methods of actualization of the actual *Attack* by *the Attacker*. If it turns out that in order to achieve *the Objectives* by any imaginable way of actualization of the attack *the Attacker* requires resources (financial, time, organizational) which exceed reasonable parameters, *the System* is declared safe against the actual *Attack*. To assess the safety of *the System* as a whole it is necessary to conduct such an analysis for all the pairs (*Victim user — Attacker*) and all the *Attacks*. Notice here, that when assessing the safety of the system as a whole, generally speaking, *each* user of the system must be regarded as a potential *Victim*, and as a potential *Attacker*!

Proposals for the rectification of security, stability and resiliency concepts in accordance with the ICANN mandate

The use of the abovementioned formal approach for assessment of the global Internet infrastructure security, in our view, would largely

put an end to an international debate and with the good will (interest) of all political actors steer these discussions toward a meaningful activity.

Let's elaborate, what would be the consequences if we apply the given methodology to assessment of security of the global infrastructure for unique identifiers, numbers and Internet settings distribution, in accordance with the multi-level model of the Internet infrastructure.

1. The distribution system (the Global Infrastructure) of unique identifiers, numbers and Internet settings is primarily an information system. And there can be multiple information systems, since in accordance with the multi-level representation of the infrastructure, on the application-level this refers to the domain name system, and for the network and transport layers — to autonomous systems' numbers, IP-addresses and port numbers. And like any information system, it, generally speaking, implements/provides an opportunity to realize the full feature set required for processing, distribution, storage, retrieval and provision of information.

- In this case «information» is understood to be the data about unique identifiers, numbers and Internet settings, as well as all service (auxiliary) information necessary to perform the functions listed above. In the definition of «security» given in the ICANN bylaws, the term «misuse» should be attributed to each of these functions.
- Elements of the system include ICANN (IANA), the structure of 13 root servers and their mirrors, including a set of functions performed by VeriSign, five Regional Internet Registries, National and Local Internet Registries (NIR, LIR), service providers, etc. Description of the system elements includes:
  - ◊ a role in processing of a particular type of information (domain names, autonomous system numbers, IP-addresses and port numbers);
  - ◊ a description of technical means of realizing the functions of the system (hardware, firmware, software);
  - ◊ a set of technical and organizational standards, regulations and procedures;
  - ◊ notes of the jurisdiction under which elements of the system are functioning.

2. Users — everyone who is a stakeholder, just as it is understood in the current discussions:

- subjects of international law: states, coalitions and alliances of states, nonstate autonomies, etc.;
- business (national, transnational, etc.), including the business associated with the Internet infrastructure;

- actors of civil society: political parties, Churches, Religions and their sects (possibly with extremist objectives), institutionalized social movements, informal unions and associations of scientists and engineers, etc.;
- informal virtual groups of Internet users with common interests («Anonymous», online games players, participants of forums, and so forth.);
- formal and informal associations of developers and engineers who are shaping the Internet (ISOS, IETF, etc.);
- citizens and individuals (among them inevitably are citizens with criminal intents).

3. Security threats to information system in the «classic» understanding include the threats against the «triad» of properties:
- Confidentiality;
- Integrity;
- Availability.

In our case, it may seem that the first of the threats — to confidentiality — is not relevant, at least in regard to unique identifiers, numbers and Internet settings (because it is difficult to imagine the reason why anyone would need to «classify» IP-address or the host name). However, the service information used in these systems can contain commercial secrets or personal data. Therefore, in this case it is necessary to ensure all the properties — confidentiality, integrity and availability.

Account must be taken of that, firstly, these threats must be correlated with the levels of the Internet infrastructure model and while at the application level we are talking about the security of the domain and of all domain name servers (DNS), at the network and transport level the frontmost objective is to ensure routing in LANs and at the level of interaction of autonomous systems.

And secondly, in this context, it is necessary to consider another aspect. Most elements of the infrastructure in question are commercial organizations, and their main objective is to gain profit. Therefore, one must keep in mind the threats to availability and integrity posed by the «withdrawal» from the system (termination or limitation of activity) of its individual parts due to a variety of external (bankruptcy, the court's decision, sanctions, revolutions, etc.) and internal (low profitability, change of the scope of activity, political or moral motivation, etc.) factors.

4. Resources available to the Attacker (and it can be any of the stakeholders!) to fulfill the objectives (i.e. to compromise the integrity and/or availability of unique identifiers, numbers and parameters as-

signed to or used by the Victim) are to a great degree determined by who the Attacker is. In particular, the central\key elements of the system (providers, registrars, controllers, etc.) have the greatest capacity and attacks by them will have the most severe consequences. And therein, apparently, lies the most «controversial» and «delicate» moment. For example, it is now obvious that it will be impossible to ignore and silence the stakeholders' distrust of hardware and software that ensures the implementation of the key functions of the system. The same applies to the cryptographic frameworks implemented by VeriSign.

Generally speaking, each of the stakeholders forms his own security threat model, according to his priorities. Nation-states and business structures, as a rule, do it explicitly, in the form of a regulatory document (public or classified); common users «are aware of» what may be dangerous for them, while many of them don't even think this subject over and «follow the lead». It is obvious, that the threat models of different stakeholders will mostly contradict each other. Apparently, the most pragmatic approach to resolve these contradictions and misunderstandings, is to use the methodology described above and develop through negotiation a set of missing «checks and balances» for the interests of the users. For example, it is possible to «balance» distrust of certain technical elements of the system with the adoption of a legal instrument, which will oblige to provide a guarantee of safety of these elements, etc.

Bibliography

[1] *ICANN's FY 14 Security, Stability and Resiliency Framework*; https://www.icann.org/public-comments/ssr-fy14-2013-03-06-en

[2] *Critical Terminology Foundations 2. Russia-U.S. Bilateral on Cybersecurity policy report 2/2014*; James B.Godwin III, Andrey Kulpin, Karl Frederick Rauscher and Valery Yaschenko (Chief Editors); https://dl.dropboxusercontent.com/u/164629289/terminology2.pdf

[3] *NISTIR 7298 Revision 2 Glossary of Key Information Security Terms*; Richard Kissel, Editor; Computer Security Division Information Technology Laboratory; May 2013; http://dx.doi.org/106028/NIST.IR.7298r2

[4] *Закон Российской Федерации «О безопасности» № 2446-I* (с изменениями от 25 декабря 1992 г., 24 декабря 1993 г., 25 июля 2002 г., 7 марта 2005 г., 25 июля 2006 г., 2 марта 2007 г.); http://www.scrf.gov.ru/documents/20.html

[5] Соглашение между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности; 16 июня 2009 г.

[6] http://www.cryptography.ru

[7] Internet Governance and the Domain Name System: Issues for Congress; Lennard G. Kruger Specialist in Science and Technology Policyб November 26, 2014, Congressional Research Service, 7-5700, www.crs.gov R42351

[8] Струков А.В.; Анализ международных и российских стандартов в области надежности, риска и безопасности; http://szma.com/standarts_analysis.pdf

[9] Пятый международный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении информационной безопасности и противодействия терроризму», 25–28 апреля 2011 г., Гармиш-Партенкирхен, Германия

[10] The Tallinn Manual on the International Law Applicable to Cyber Warfare, http://www.cambridge.org/ca/academic/subjects/law/humanitarian-law/tallinn-manual-international-law-applicable-cyber-warfare

[11] NATO Cooperative Cyber Defense Centre of Excellence free e-book entitled «Peacetime Regime for State Activities in Cyberspace», including a chapter on Space Law and Unauthorized Cyber Activities. https://ccdcoe.org/multimedia/peacetime-regime-state-activities-cyberspace.html

Чарльз Барри

Центр политики в области технологий и национальной безопасности, Университет национальной обороны, США[1]

Интернет-уязвимости крупных организаций: Исследование отказоустойчивости уровня автономных систем[2]

Краткое содержание

В настоящей работе проводится анализ устойчивости и уязвимостей подключений крупных организаций к Интернету. В ней содержится исследование зависимостей общественных организаций и частных предприятий, деятельность которых в значительной степени зависит от Интернета. Схемы как логических топологий, так и физических структур Интернета легко найти. Однако логические топологии информационных потоков находятся в постоянном движении, и визуальные графики отображают только конкретные наносекунды реального подключения. Физическая основа связей и узлов, по которым передаются данные, менее подвижна, но она тоже постоянно меняется по мере возникновения новых структур и изменения деловых отношений между поставщиками. Эти логические и физические карты являются взаимозависимыми.

Автономные системы (AS) являются основными структурными элементами подключения к Интернету, и они включают в себя уровень сети с наиболее полезной информацией для детального анализа. Маршруты Интернет-трафика определяются логикой (политикой) маршрутизации, используемой различными AS-сетями, участвующими в передаче любых данных, а также сетью физических связей, имеющихся между отправителем и получателем этих данных. Выводы и рекомендации, приведенные в сле-

[1] Д-р Чарльз (Чак) Барри проводит консультации для частного сектора в Университете Национальной обороны. Настоящий доклад, в том числе заключения и рекомендации являются его собственными и не отражают взглядов, позиций или официальную политику Университета Национальной обороны, Министерства обороны или правительства США.

[2] Настоящая статья основана на модификации неопубликованного исследования, проведенного в 2012–2014 гг. в Университете Национальной обороны, совместно с Др. Лин Уэллс, которое, в свою очередь, основано на более ранней работе Терри Пудаса и Дэвида Кэя. Все мы работали в то время в Центре политики в области технологий и национальной безопасности.

дующей обзорной части этой статьи, основаны на этом анализе уровня автономных систем.

Коммерческие сервисы и научные исследования дают обширные сведения об отказоустойчивости подключений к Интернету отдельных организаций. Некоторые исследования показывают, что устойчивость ведущих организаций не так надежна, как у лучших компаний отрасли. Тем не менее, необходим более подробный анализ для того, чтобы выявить какую-либо полезную информацию об уязвимостях и предложить конкретные средства защиты. Полноценное исследование может указать на необходимость большего резервирования физических соединений, целесообразность индивидуальной политики маршрутизации для каждого заказчика и контрактных соглашений с несколькими поставщиками услуг или даже международных инициатив, направленных на укрепление областей физической инфраструктуры с высоким риском отказов в единой точке.

Из результатов такого анализа следуют еще два направления исследований. Первое должно основываться на моделировании и эмуляции с целью лучшего понимания того, как логическая топография Интернета реагирует на изменения в своей физической структуре. Это может быть сделано как с использованием существующих, так и путем разработки новых моделей и методов моделирования. Вторая линия исследований должна основываться на взаимодействии с внешними научными и коммерческими предприятиями, которые уже ведут анализ метаданных транзитного трафика; итогом должно стать понимание того, какая информация должна быть дополнительно рассмотрена для получения высокоточной картины организационных зависимостей и, соответственно, уязвимостей к сетевым сбоям. Обе эти инициативы могут дать более глубокое понимание возможных средств решения проблем.

Обзор

Практически все организации зависят от Интернета для удовлетворения своих жизненно важных информационно-коммуникационных потребностей, а также для осуществления ежедневных деловых операций. Таким образом, подключения к Интернету являются критически важными. Надежность требует разнообразия вариантов доступа и резервирования, безопасной топологии исходящего трафика во всей инфраструктуре Интернета.

Логические и физические «карты» Интернета являются взаимозависимыми, и обе очень динамичны. Политики маршрутиза-

ции используют алгоритмы, основанные на таких критериях, как объем информации, кратчайший путь к получателю, стоимость транзита, доступность сети и пиринговые отношения. Политики маршрутизации регулярно пересматриваются поставщиками Интернета без предварительного уведомления. Варианты физической маршрутизации могут резко измениться ввиду таких реалий, как отказ оборудования, задержки, скорость передачи через подводные или наземные кабели и перегрузка точек обмена Интернет-трафиком. Логическая *не*доступность конкретных соединений и узлов является ключевым фактором физической маршрутизации.

Таким образом, в центре внимания здесь находится уровень автономных систем Интернета. Автономные системы, которые представляют интерес, это тысячи провайдеров транзитных услуг (Интернет-провайдеры). Они находятся на узлах Интернета и между ними, там, где определяются политики маршрутизации, управляющие соединениями внутри и между многоуровневыми сетями, составляющими Интернет. Разнообразие и избыточность этих соединений либо представляют собой картину избыточной надежности, либо картину, в которой есть от нескольких уязвимостей до, возможно, нарушенной функциональности. Физические связи Интернета также наиболее ярко проявляются на уровне автономных систем. Основными составными элементами являются кабели и точки обмена трафиком (ТОТ), в которых провайдеры осуществляют обмен трафиком между сетями. ТОТ часто находятся там, где соединяются основные сухопутные и подводные кабели. Любые перебои в работе этих узлов и соединений представляют собой физическую сторону потенциальных уязвимостей данных во время передачи.

Мониторинг и детальное картографирование Интернет-трафика осуществляется исследовательскими центрами и сервисами отслеживания данных в Интернете. Подобные предприятия специализируются на точной ситуационной осведомленности о перегрузках соединений, отключениях оборудования и таких разрушительных событиях, как стихийные бедствия и вредоносные атаки. Отслеживание информации может быть адаптировано к коммерческому использованию, особенно в финансовой и энергетической отраслях, или для государственных ведомств, например, министерств иностранных дел и министерств обороны.

Логические карты информационных потоков изображаются как потоковые графики или снимки, как правило, в масштабе миллисекунд. Они показывают нормальный или меняющийся

объем трафика, и отображают разрушительные события, которые мешают потоку трафика. Например, сервис мониторинга Интернет-трафика Renesys (в настоящее время приобретен корпорацией Dyn) опубликовал несколько последовательных графиков, изображающих нарушение Интернет-трафика в Таиланде во время недавних протестов[3].

Большая часть физической инфраструктуры Интернета надежна и продублирована, однако не всегда безопасна. Первичный анализ показывает, что во многих областях, представляющих интерес, разнообразие может быть улучшено (в приложениях 2 и 3 рассмотрены уязвимости подводных кабелей и Интернет-провайдеров). Тем не менее, при выборе путей маршрутизации в игру вступают многие другие факторы, в том числе политика, деловые соглашения, цена транзита и конфигурация маршрутизатора.

В настоящем исследовании рассматривается несколько комбинаций физических инфраструктур и логических топологий. Полезная метрика рассматривает различные уровни (1, 2 или 3) непосредственных поставщиков доступа и количество различных поставщиков, доступных организации, и показывает общую картину разнообразия и устойчивости транзита в случае сбоев в обслуживании. Рекомендации включают в себя изменение политики компаний и обсуждение лучших условий обслуживания для повышения устойчивости зависимых от Интернета сетей во всем мире.

Логические топологии дают представление о потенциальных уязвимых точках, связанных с такими общими факторами, как повышенный объём трафика. Логические топологии могут быть отображены многими способами. Узлы могут быть показаны по объёму контента или числу соединений. Толщина линий, показывающих связи, может отражать нормальный объем передаваемого трафика. Карты могут демонстрировать маршруты передачи пакетов в виде моментального снимка. Эти визуализации могут быть очень интересными, даже эффектными, но ни одна из тех, которые были рассмотрены, не дала полезной информации о поддержании устойчивости сети.

Наиболее распространенными причинами физического нарушения работы сетей всё еще являются случайные повреждения, поломки оборудования или преступная деятельность. Политически мотивированные нападения на Интернет-инфраструктуры

---

[3] См. Doug Madory, *Protest Leads to Outage in Thailand*, 7:56 pm, 2 декабря 2013 по адресу http://www.renesys.com/2013/12/protests-lead-outage-thailand/

встречаются гораздо реже, но их число возрастает. Своевременные меры по определению транзитных зависимостей, системных уязвимостей и резервированию доступа могут помочь любой зависимой от Интернета организации оценить, на что выделять ресурсы для повышения надежности.

Настоящее исследование не рассматривает все риски, присущие зависимости от Интернета. Уровень автономных систем не включает в себя уязвимости, которые могут присутствовать на уровне подсетей *внутри* каждой автономной системы. Применение маршрутизаторов в пределах подсетей (иногда тысячи маршрутизаторов) может создавать другие единые точки отказа, которые не видны на уровне самой автономной системы. Дальнейшие исследования могут обнаружить другие физические или логические уязвимости, и многое еще предстоит сделать для того, чтобы определить оптимальный уровень устойчивости соединений. Для очень больших организаций с глобальными деловыми интересами, возможно, будет необходимо детализировать и определить приоритеты зависимостей для каждого из своих подразделений, чтобы более подробно рассмотреть наиболее критические уязвимости; например, по географическим регионам, и приоритизировать объекты в этих областях.

Выводы, рекомендации и дальнейший анализ

Высокая устойчивость доступа помогает обеспечить непрерывную связь и предохраняет от нарушений работы. Снимков сетей в один момент времени или в одной точке недостаточно. Организации должны обладать непрерывной осведомленностью о состоянии своих непосредственных подключений к Интернету, а также о системной надежности соответствующих автоматизированных систем, находящихся на более высоком уровне. Такая ситуационная осведомленность должна простираться за пределы самых общих транзитных путей организации и включать в себя понимание общей физической инфраструктуры Интернета и логических топологий, участвующих в маршрутизации трафика в сетях от пункта отправления до пункта назначения — в том числе понимание потенциальных уязвимостей в логических путях, которые могут происходить от многих источников. Определение надлежащей связи требует стандартов, которые постоянно развиваются, и не могут быть в полной мере определены. Отказоустойчивость также может потребовать таких новых инициатив, как государственно-частное партнерство, общеправительственное участие и двусторонняя дипломатия.

Рекомендации

- Выявить автономные системы, которые имеют решающее значение для стратегической и оперативной связи организации.
- Разработать высокоточную методологию непрерывного мониторинга Интернет-зависимостей.
- Взаимодействовать с государствами и поставщиками из частного сектора в Соединенных Штатах и за рубежом, чтобы повысить связность и безопасность хотя бы критически важных сетей.
- Выработать международные инициативы, которые помогли бы государствам, в которых размещены узлы, в устранении недостатков инфраструктуры и уязвимостей.
- Проанализировать контракты с Интернет-службами и политики маршрутизации, чтобы снизить уязвимости и повысить способность быстрого перенаправления сетевого трафика, когда/где происходят сбои.
- Что касается поставщиков облачных услуг, убедиться, что резервные данные и системы не хранятся в одном облаке.
- Быть осведомленными о глобальных кризисах, которые могут потребовать перенаправления трафика компании через страны, где он не будет нарушен.

Области для дальнейшего анализа

- Изучить методологии для измерения устойчивости подключения к Интернету, чтобы определить лучшие метрики для постоянного мониторинга.
- Провести анализ связей основных субагентств, учреждений и критически важных сайтов и сравнить их устойчивость с приемлемыми показателями.
- Разработать методологию для определения автономных систем, стран и регионов, где глобальная организация имеет наибольшую уязвимость / наименьшую устойчивость.
- Объединить их в более детальном анализе устойчивости по регионам и функциям.
- Разработать систему непрерывного мониторинга отказоустойчивости, например, системы показателей, для каждой командной структуры, учреждения, поля деятельности, критического сайта во всем мире.
- В глобальном масштабе выявить и установить профили риска для каждой критически важной точки обмена Интернет-трафиком, подводных и сухопутных кабелей, мест выхода кабелей на поверхность, крупных центров обработки данных и спутниковых станций, которые уязвимы для физического разрушения.

Основная часть

Интернет можно рассматривать как глобальную инфраструктуру информационно-коммуникационных технологий (ИКТ) — взаимосвязанную сеть ячеек, состоящую из маршрутизаторов, коммутаторов и других специализированных узлов, соединяющих компьютеры и другие информационные системы. Двумя ключевыми компонентами ИКТ-инфраструктуры являются ее глобальная физическая архитектура и логическая топология. Физическая инфраструктура состоит из материальных структур и оборудования, расположенных на территории страны или в космическом или подводном пространстве, которое является всеобщим достоянием. Большая часть этой физической инфраструктуры эксплуатируется частными лицами. Логическая топология сети Интернет определяется политиками маршрутизации (программные протоколы или наборы правил) установленными каждым из администраторов тысяч отдельных доменов (сетей), называемых автономными системами[4], для того, чтобы контролировать скорость передачи и маршрут информации внутри соответствующих автономных систем и между ними.

Настоящее исследование посвящено логическому картографированию Интернета на уровне автономных систем и основано на работе, проделанной такими компаниями, как Dyn (ранее Renesys) и Научной группой сетевых исследований университета Луизианы — Lafayette. Моделирование уровня автономных систем производится для создания топологического рисунка, который является более подробным, чем отображение сетевого уровня, однако более агрегированным, чем тот, который получается при анализе уровня подсетей или маршрутизаторов. Все уровни моделирования имеют значение, и каждый из них предлагает дополнительную точку зрения на топологию маршрутизации. В конечном счете, помимо описания уровня автономных систем, понадобятся дополнительные модели для понимания зависимостей в Интернете и оценки разнообразия доступа для

---

[4]Автономная система представляет собой набор маршрутизаторов, работающих под единой технической администрацией и использующих протокол внутреннего шлюза и общие показатели для определения маршрута пакетов внутри автономной системы и пограничный межсетевой протокол для определения маршрутизации пакетов к другим автономным системам. См. документ RFC 4271 Инженерной рабочей группы Интернета, под ред. Rehkter, Y., Li, T., Hares, S. «A Border Gateway Protocol 4,» Network Working Group/Standards Track, The Internet Society. January 2006. Стр. 4. http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_9-1/autonomous_system_numbers.html

различных суборганизаций. Например, полноценное определение устойчивости сети требует анализа нижестоящих подсетей и маршрутизаторов, а также связей с вышестоящими точками обмена Интернет-трафиком. Настоящее исследование является только началом работы.

Интернет не является неизменной «сетью сетей». Количество и размер сетей, определяемых автономными системами, постоянно меняется. В настоящее время (на 12 декабря 2013 года[5]) систему маршрутизации Интернет-протокола версии 4 составляют более 45800 автономных систем. Они работают через 300 (или более) крупных точек обмена Интернет-трафиком[6] и небольших узлов связи, а также через более чем несколько сотен тысяч миль подводных и наземных волоконно-оптических кабелей, космических и микроволновых линий передачи данных.

Автономные системы часто представляют собой Интернет-провайдеров (ISP)[7], обеспечивающих передачу данных между хостами. Провайдеров в свою очередь можно характеризовать как поставщиков услуг 1, 2 или 3 уровня. Провайдерами первого уровня являются те, которые могут получить доступ к любой части Интернета самостоятельно или через пиринговые сети, и которым для этого не требуется приобретать транзит или выплачивать пиринговые взносы другим провайдерам. В Соединенных Штатах в тройку ведущих провайдеров первого уровня входят Level 3 Communications, Verizon Business и AT&T[8]. В других регионах провайдерами первого уровня являются, в том числе, NTT Communications (Япония), China Telecom, Tata (Индия), Deutsche Telekom AG (Германия), TeliaSonera (Европа) и Seabone (Италия)[9]. Эти одноранговые автономные системы, как правило,

---

[5] См. доклад Classless Inter-Domain Routing (CIDR) по адресу http://www.cidr-report.org/as2.0/

[6] Это количество точек обмена Интернет-трафиком взято у корп. Telegeography, См. текущую карту по адресу: http://www.telegeography.com/telecom-resources/internet-exchange-map/index.html

[7] Провайдеры Интернета являются коммерческими автономными системами, предоставляющими услуги доступа в Интернет. В то время как все провайдеры являются автономными системами, не все автономные системы являются провайдерами. Например, Центр сетевой информации Министерства обороны США имеет как минимум четыре автономные системы (AS 721, AS2706, AS27065 and AS27066). См. http://bgp.he.net/AS721

[8] Глобальная география Интернета, Стр. 10. См. http://www.telegeography.com/page_attachments/products/website/research-services/global-internet-geography/0003/1871/GIG_Executive_Summary.pdf

[9] См. http://drpeering.net/FAQ/Who-are-the-Tier-1-ISPs.php

имеют наибольшую мощность, самые современные технологии и самую сильную устойчивость. Их часто неофициально называют «опорными сетями Интернета»[10].

Провайдеры второго уровня обмениваются трафиком с другими провайдерами, а также приобретают права на транзит в других частях сети Интернет от других Интернет-провайдеров, как правило, первого уровня. Провайдеры третьего уровня обеспечивают транзит в Интернете только через соглашения, которые они покупают у других провайдеров. Этот третий уровень является типичной точкой доступа для физических лиц и малого бизнеса. Для повышения качества обслуживания, а также охвата и надежности крупные организации могут и должны напрямую подключаться к автономным системам (Интернет-провайдерам) первого или второго уровня.

Постоянно меняющийся состав автономных систем Интернета затрудняет создание точной, актуальной карты его структуры в традиционном смысле. Благодаря использованию программ трассировки, а также других показателей, ряд коммерческих компаний может обеспечить поминутное картографирование, особенно там, где оно накладывается на такие известные географические ориентиры, как границы конкретного государства. Провайдеры в пределах страны или региона могут быть определены, а крупнейшие поставщики услуг относительно зафиксированы с точки зрения их статуса 1 или 2 уровня. Доля рынка или «охват» каждого Интернет-провайдера, определяется процентом адресов Интернет-протокола (IP), обслуживаемых ими с помощью нижестоящих провайдеров.

Физическая инфраструктура Интернета

Физическая инфраструктура Интернета состоит из доменных сетей автоматизированных систем — первого, второго и третьего уровня, как описано выше.

В крупных точках обмена Интернет-трафиком порядка 50 или 60 автономных систем поддерживают связь друг с другом в одном здании. Там они могут подключаться к нескольким автономным системам или провайдерам подводных кабелей для передачи трафика. Такие точки обмена трафиком, как дом 60 по Гудзон-стрит и дом 111 на восьмой авеню в Нью-Йорке или дом 530 на шестой стрит в Лос-Анджелесе являются одними из самых крупных, но

---

[10] Джефф Тайсон, How Internet Infrastructure Works, http://computer.howstuffworks.com/internet/basics/internet-infrastructure2.htm

подобные типы узлов существуют во всём мире, и более чем 250 доступны для анализа через интерактивные карты. Если передача трафика прервется в любой из этих точек, это потребует альтернативной маршрутизации. В некоторых местах, например, Соединенных Штатах, альтернативная маршрутизация может быть легко установлена, но в другом месте, например, в Центральной Азии, сделать это может быть гораздо сложнее. В любом случае, некоторые точки обмена Интернет-трафиком[11] могли бы стать привлекательными целями для того, чьей целью является нарушение Интернет-трафика, и многие из них не очень хорошо защищены от физических атак.

Примерно 95% Интернет-трафика передаётся через волоконно-оптические линии связи, либо в наземных, или подводных кабелях. Оставшиеся 5% (или менее) передаются через спутники, микроволновые линии, атмосферные оптические линии связи и другие нишевые средства. Волоконно-оптические кабели попрежнему намного эффективнее спутников в плане эксплуатационных расходов, пропускной способности, качества сигнала и надежности[12]. Однако спутники обеспечивают важную альтернативу по предоставлению услуг при возникновении нештатных ситуаций и осуществлении высокоприоритетных передач в отдаленных районах. С 2011 года новое поколение спутников повысило скорость и надежность Интернет-соединения при более низкой стоимости, чем предыдущие спутниковые системы[13]. Ожидается, что эта тенденция получит развитие.

Третьим важным компонентом физической инфраструктуры, хотя и косвенным, является энергосистема, так как узлам и соединениям необходимо электричество[14]. Электрические сети, хотя и не обслуживают исключительно Интернет, должны быть рассмотрены при оценке уязвимости. Инфраструктуры ИКТ и энергетики идут рука об руку и являются двумя наиболее экономически важными инфраструктурами в любой стране.

---

[11] См. Карту Интернет-обмена корп. Telegeography по адресу: http://www.internetexchangemap.com

[12] http://www.fiercetelecom.com/special-reports/submarine-cable-operators-hunt-new-routes-counter-congestion-political-turm

[13] См. Доклад Федеральной комиссии связи от февраля 2013 г. по адресу: http://www.fcc.gov/measuring-broadband-america/2013/February

[14] Например, один из узлов Интернета, крупнейший дата-центр по адресу 350 East Cermak Ave в Чикаго является крупнейшим потребителем электроэнергии в городе после международного аэропорта О'Хара. Подводные кабели, как правило, требуют 3–4 КВт энергии для работы усилителей сигнала.

Логическая топология сети Интернет определяется архитектурой маршрутизации, основанной на политиках, протоколах и наборах правил, установленных и поддерживаемых автономными системами. Наиболее значимым набором протоколов Интернета является двойной протокол, называемый TCP/IP (протокол управления передачей/межсетевой протокол). TCP/IP определяет то, как данные должны форматироваться, адресоваться, передаваться, направляться и приниматься. Он является фундаментальным протоколом, который определяет порядок сквозного соединения в системе сетей Интернета.

Другим основным протоколом является протокол пограничной маршрутизации (Border Gateway Protocol — BGP), который автономные системы используют для определения своей политики маршрутизации с доменами друг друга. TCP/IP, BGP и многие другие протоколы определяют логику Интернета. Автономные системы также используют протокол внутреннего шлюза (Interior Gateway Protocol — IGP) для внутренней маршрутизации между своими IP-подсетями. Важно отметить, что автономные системы закономерно отдают предпочтение маршрутизации трафика через свои собственные подсети, «сестричные» узлы или одноранговые сети, с которыми они имеют соглашения о маршрутизации. Это может означать более протяженные, чем ожидается, маршруты в некоторых ситуациях маршрутизации. Для простоты анализа будем считать автономные системы едиными компаниями в рамках логики маршрутизации Интернета в целом.

Среди наиболее значимых приложений логического Интернета выделяются операционные системы физических соединений и узлов; программное обеспечение, используемое провайдерами различных уровней; и программное обеспечение системы доменных имен (DNS). Как и протоколы, которые они используют, эти системы влияют на потоки трафика в Интернете.

Армия сетевых администраторов, которые устанавливают различные политики маршрутизации для своих автономных систем, также оказывает значительное влияние на логику потока трафика своих клиентов. Сейчас существует около 72000 выделенных номеров в автономной системе (Autonomous System Numbers)[15], каж-

[15] См. http://www.potaroo.net/tools/asn32/. Как указано на этом сайте, 71,678 номеров в автономной системе были присвоены региональным Интернет-регистраторам на 2 июня 2013 года. Не все из них были присвоены автономным системам (в системе маршрутизации около 42000 активных автономных систем).

дый с определенным набором политик внешней маршрутизации. Эти политики определяют нормальную маршрутизацию потоков, а также то, как будут перенаправлены потоки трафика в случае перебоев или в чрезвычайных ситуациях. Например, для трафика своих крупнейших клиентов Интернет-провайдеры могут устанавливать первостепенный приоритет в плане пропускной способности, скорости передачи и восстановлении после сбоев. В то время как физические карты сетей, как правило, доступны через открытые источники, чтобы информировать пользователей о потенциальных рисках снижения качества обслуживания, администраторы сетей частного сектора, как правило, считают фактические (в сравнении с начальными) политики маршрутизации своих систем, и, таким образом, большую часть детализации логической топологии Интернета, закрытой информацией.

Интернет-уязвимости

Эта статья посвящена не проблеме кибербезопасности, но некоторая справочная информация о потенциальных уязвимостях и типах физических и логических сбоев может оказаться полезной.

Физические и логические сбои могут возникнуть в результате природных или техногенных причин, случайных или преднамеренных, а также по причине электромеханических сбоев (в том числе перегрузки системы). Физические нарушения могут привести к логическим, и наоборот: физическое повреждение сетевого компонента может изменить логический поток, что может повлиять на задержки и пропускную способность сети. В преддверии военных действий можно ожидать нарушения (по крайней мере, временного) ключевых коммуникаций и информационных узлов путем физического прерывания связи, постановки помех или иными способами. Кроме разрушения инфраструктуры в Нью-Йорке в связи с событиями 11 сентября, теракты до сих пор не вызвали значительного нарушения функционирования Интернета (в отличие от повреждения таких целевых объектов, как НПЗ

Большая часть номеров — более 63 000 — это старые 16-битные номера. Автономная система может работать более чем с одним номером. В 2011 году началось распределение более новых 32-битных номеров. Механизма возврата более не используемых или не нужных номеров не существует. Таким образом, этот номер должен рассматриваться как приблизительное количество политик маршрутизации, используемых в Интернете, однако, принимая во внимание полученное число, картографирование будет весьма сложным процессом. Отмечается, что этот вебсайт обновляется ежедневно.

Aramco в Саудовской Аравии); но это должно рассматриваться как будущая возможность.

Нарушение логической топологии посредством вредоносных программ может нарушить/снизить качество физической составляющей Интернета, например, атаки типа распределенный отказ в обслуживании (DDoS) нарушают работоспособность серверов. Точками уязвимости для логического Интернета являются: (1) манипуляции с программным обеспечением TCP/IP, (2) атаки, направленные на Интернет-провайдеров, и (3) атаки на саму DNS. Более подробная информация содержится в Приложении 3.

Ключевым моментом является то, что по-настоящему глобальная стратегия снижения уязвимостей не может носить в основном технический характер; должен присутствовать интегрированный государственно-частный, общеорганизационный и общеправительственный транснациональный подход, одинаково затрагивающий людей, процессы, организации и технологии.

Анализ зависимостей

Измерение устойчивости к нарушениям связи в Интернете

Измерение устойчивости организации к нарушению связи в Интернете требует понимания альтернативных средств передачи информации, которые могут быть использованы в случае недоступности конкретной части Интернета. Это важно, поскольку передача большей части информации любой крупной организации, в том числе обмен закрытыми данными, осуществляется через сети общего пользования, или, точнее, инкапсулируется, шифруется и туннелируется[16] через инфраструктуру Интернета. Анализ зависимости от Интернета должен включать в себя: (1) важность подсети, (2) профиль принимающей страны, (3) разнообразие доступных соединений.

Важность: Какие части и регионы сети Интернет являются наиболее важными для организаций и зависимость от какой части этой инфраструктуры и логической топологии представляет

[16] Туннелировние или «переброска портов» является стандартной техникой защиты информации для многих Интернет-пользователей. Существует множество протоколов и методов для инкапсуляции или шифрования данных в небезопасных сетях, например, протокол туннелирования точка-точка компании Майкрософт (PPTP) или протокол безопасной оболочки (SSH). Туннелирование создаёт виртуальную частную четь для авторизованных пользователей. См. http://searchenterprisewan.techtarget.com/definition/tunneling

собой неприемлемый риск? Важно будет выявить, на какие автономные системы опирается организация, сколько из них принадлежит одному провайдеру, где находятся ключевые узлы и соединения и какие политики маршрутизации они используют. Должны быть выставлены приоритеты для, например, автономных систем, обслуживающих штаб командования, и тех, которые обслуживают не передовые подразделения, находящиеся в удаленных местах. Аналитики также должны понимать доступную избыточность. В конечном счете подобные показатели будут необходимы для критически важных для национальной безопасности межведомственных партнеров и союзников.

Профиль принимающей страны: Организациям также необходимо знать профиль инфраструктуры Интернета в принимающих странах, в которых они работают или планируют работать в будущем. Количество в стране номеров автономных систем (НАС), присвоенных международным соглашением, как правило, Интернет-провайдерам, является одним из признанных показателей надежности инфраструктуры Интернета. Например, в Турции, как сообщается, 290 НАС, а в Азербайджане только 31. Среди других стран, которые можно отметить, Афганистан со всего двадцатью и Туркменистан с только лишь двумя. Сирия, как предполагается, также обладает только двумя НАС, в то время как Йемен имеет только одну. Эти цифры указывают на страны, которые подвержены риску значительных нарушений в случае природных или антропогенных катастроф. Среди других стран, которые имеют мало, или вообще не имеют собственного доступа в Интернет, Бангладеш, Туркменистан, Узбекистан, Ливия, Северная Корея и Куба[17].

Разнообразие путей передачи: Каким разнообразием путей передачи информации обладает та, или иная организационная подструктура на пути к провайдерам Интернета верхнего уровня? Имеются ли подключённые альтернативные провайдеры и каналы, готовы и в состоянии ли они поддерживать непрерывность соединения на случай выхода из строя основного провайдера,

---

[17] Цифры актуальны на январь 2013 года. Номера автономных систем присваиваются Управлением по присвоению Интернет-номеров для пользования протокола пограничной маршрутизации (протокол пограничной маршрутизации является протоколом ядра внутри протокола TCP/IP). Автономные системы в стране обычно являются Интернет-провайдерами, а число номеров автономных систем в одной стране является одним из показателей устойчивости Интернет-инфраструктуры. См. http://www.renesys.com/tech/presentations/pdf/menog12-cowie.pdf

узла или соединения? Это более глубокий вопрос, чем просто количество автономных систем, непосредственно обслуживающих каждую критически важную сеть любой ТНК или глобальной организации. Чтобы понять, сходятся ли несколько автономных систем в какой-то одной точке уязвимости, ответ должен включать в себя анализ вышестоящих провайдеров и архитектуры маршрутизации на всем пути до опорных сетей Интернета. Деловые отношения между поставщиками Интернета находятся в постоянном движении, а вместе с ними изменяется архитектура маршрутизации связанных автономных систем. Эффективный аналитический процесс должен включать в себя постоянную связь с поставщиками услуг и принимать во внимание периодические обновления маршрутизации.

Устойчивость является функцией разнообразия путей передачи, которое достигается не только использованием нескольких прямых провайдеров автономных систем, но также путем обеспечения нескольких путей к вышестоящим косвенным провайдерам на всём маршруте к опорным сетям Интернета. В дополнение к оценке прямых и косвенных связей провайдеров с каждой из своих подчиненных структур, каждая глобальная организация должна быть в курсе деловых отношений своих Интернет-провайдеров. Используют ли некоторые или все поставщики одну и ту же материнскую автономную систему? Уязвимы ли критически важные автономные системы к нарушениям взаимного обмена, которые могли бы затруднить их соединения с клиентами или сотрудниками? Если это так, нарушение работы в масштабах организации может отразиться во всех автономных системах, обслуживающих одно или несколько соединений.

Недавний анализ компании Dyn/Renesys был посвящен маршрутизации данных на уровне автономных систем, его целью было оценить прямое и косвенное разнообразие подключений путем изучения взаимоотношений между провайдерами. Затем, они провели оценку организаций по степени разнообразия их подключений, от никакой (нулевая оценка) до значительного разнообразия без каких-либо единых точек отказа (оценка 100). График рассеяния на таблице А (см. ниже), отображает результаты десятков тысяч организаций, присутствующих в Интернете, сгруппированных по количеству используемых автономных систем (вертикальная ось). Примечательно, что Министерство обороны США (DoD), являющееся лишь одной из многих организаций, приведенных в анализе, получило низкую оценку в 34 балла, что может указывать на значительный потенциал для

улучшения разнообразия доступных подключений в её присутствии в Интернете.[18] Низкая оценка MO, вероятно, отражает картину для большой рассредоточенной организации с множеством независимых, локально законтрактованных провайдеров связи. Кроме того, результат на уровне MO в любой точке на шкале малоинформативен, поскольку не показывает, где разнообразие подключений находится на низком уровне, а где, возможно, его будет достаточно. Уязвимы ли основные командования к нарушениям связи? Там нет разбивки среди множества подчиненных командований или учреждений, занимающихся, например, логистикой, или кадровыми вопросами. Алгоритмы Renesys являются проприетарными, но возможно провести более детальный анализ данных и, это, скорее всего, будет полезно.

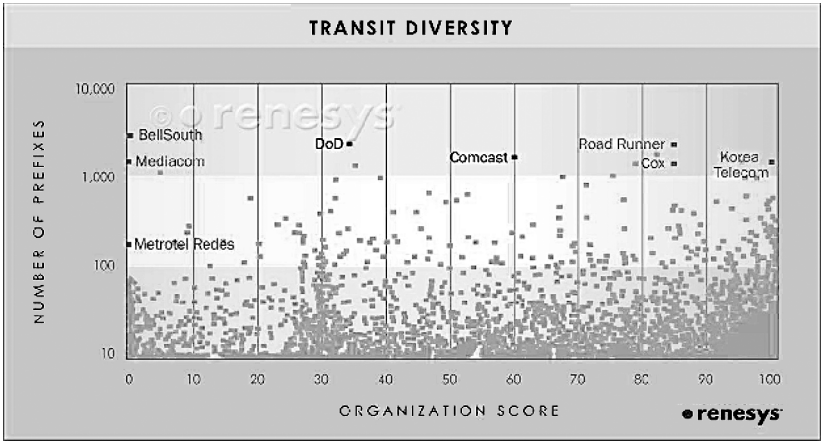


Табл. 1. Показатели разнообразия подключений Renesys

Двойственная прямая-косвенная зависимость: электро-энергетическая система

Интернет-зависимость, связанная с электро-энергетическими сетями, является как прямой, так и косвенной. Большинство организаций с критически важными сетями имеют такие резервные или аварийные источники питания, как генераторы, чтобы компенсировать перебои в подаче электроэнергии, однако некоторые из них рассматривают возможность подключения своих ключевых объектов к нескольким поставщикам энергии. Это важно, поскольку аварийный запас топлива может закончиться, а резерв-

[18] См. http://www.renesys.com/2009/05/keeping-score/

ные элементы выйти из строя. Практически все критически важные инфраструктуры Интернета управляются частным сектором. Механизмы частного сектора по поддержанию непрерывности работы инфраструктуры различаются по качеству, но большинство из них включает в себя резервное энергоснабжение, хотя и на ограниченный период времени. Таким образом, обширные продолжительные отключения электроэнергии, которые влияют на нескольких провайдеров услуг, могут привести к снижению производительности сети Интернет для многих пользователей. Нарушение электроснабжения и Интернет-соединений также может привести к невозможности потребителей оплатить такие критически важные товары, как топливо и лекарства, что чревато потенциальными последствиями для социальной стабильности.[19]

Геополитическое влияние на физический/логический Интернет

В дополнение к физическим и логическим уязвимостям, которые могли бы помешать способности организации использовать Интернет в глобальном масштабе, провайдеры за границей могут не уделять достаточного внимания модернизации инфраструктуры и безопасности. Связанной проблемой является то, что беспорядки в странах со слабым управлением или недружественными правительствами могут посредством правовых маневров или иный действий блокировать или нарушать передачу данных через Интернет в пределах своих границ.

Некоторые государства регулируют Интернет-контент и осуществляют управление телекоммуникациями через государственные компании или являются собственниками физической инфраструктуры, необходимой для подключения к сети Интернет. Авторитарные режимы также предпринимали меры по ограничению доступа в Интернет во время кризисов. Во время протестов в Египте в январе 2011 года правительство использовало положение закона о телекоммуникациях, касающееся национальной безопасности, для того, чтобы принудить иностранных провайдеров беспроводной связи отключить доступ к мобильным сетям. Большинство изначально сделало это, хотя спустя некоторое вре-

[19] Примером может служить неспособность покупателей приобрести бензин с помощью кредитных карт после урагана Сэнди. Исследование значительных событий космической погоды, проведенное в Университете Национальной обороны в 2011 году, показывает, что продолжительные нарушения энергоснабжения на обширной местности вызывают особую обеспокоенность населения по поводу распределения медикаментов.

мя услуги в ограниченном объёме были восстановлены[20]. Замысел практически не повлиял на восстание, так как протестующие совместно нашли способы обхода ограничений[21]. Тем не менее, эти действия продемонстрировали, насколько сильно некоторые государства будут стремиться ограничить доступ к неотфильтрованной информации и Интернету.

Следует предположить, что в авторитарных государствах частный (получающий прибыль) сектор, граждане и третьи лица (международные операторы Интернета и пользователи) будут мало или вообще не прибегать к юридической апелляции или законодательному регулированию против государственных действий по вмешательству в функционирование Интернета. В то же время плохая физическая или кибербезопасность также может открыть пути, которые могут нарушить или ухудшить подключение к Интернету путем не поддающихся атрибуции действий из почти любого географического региона.

Аспекты дипломатического, правового или коммерческого взаимодействия для снижения уязвимости

Дипломатическое, правовое или коммерческое взаимодействие на различных уровнях способно уменьшить уязвимости и расширить резервирование Интернета за рубежом. Наиболее важный шаг — убедить правительства отдавать безопасности и надежности информации, коммуникаций и связанных с ними инфраструктур (ИКТ), гораздо более высокий приоритет, чем сейчас. Эти возможности помогают определить победителей и проигравших в экономическом плане, оказывают влияние на международные отношения и меняют образ мышления наших детей. Тем не менее в рамках межведомственных приоритетов они редко рассматриваются как критически важные услуги или инфраструктуры. Эти вопросы касаются бизнеса и государственных

[20] См. http://latimesblogs.latimes.com/babylonbeyond/2011/01/egypt-foreign-telecomms-stepping-in-to-connect-protesters-to-internet.html. France Telecom и Vodafone Group были двумя операторами, которые восстановили обслуживание через несколько дней. Другие использовали проводную связь и старые коммутируемые службы для преодоления разрывов беспроводной связи.

[21] См. http://www.aljazeera.com/news/middleeast/2011/01/201112515334871490.html В выходные дни 30–31 января при взаимодействии Google и Twitter сервисом SayNow, приобретенным Google, был запущен бесплатный международный телефонный сервис “speak2tweet”, посредством которого пользователи в Египте могли оставить сообщение в системе Twitter. Успех этой инициативы по обходу блокировок привел к созданию аналогичных сервисов в Сирии в 2012 году, когда правительство угрожало ограничением доступа к социальным сервисам и Интернету.

лидеров и политиков, а не только операторов киберпространства. Некоторые из этих возможностей:

- Содействовать государствам, которые не имеют достаточного резервирования в пределах своих границ, чтобы увеличить диверсификацию маршрутизации, по меньшей мере для их основных каналов. Отказоустойчивость сети может быть включена в повестку дня при ведении переговоров о транзитных пошлинах.
- Участвовать в проектах новых или модернизированных волоконно-оптических наземных или подводных кабелей, которые часто осуществляются при поддержке консорциумов международных компаний и стран, которые будут обслуживаться. Можно рекомендовать многонациональным консорциумам закладывать в свои проекты такие защитные меры, как закапывание подводных кабелей, укрепление наземных точек подключения, установка передовых систем мониторинга и инвестирование в возможности надежного обслуживания.
- Проводить оценку государств, в которых располагаются центры телекоммуникационных операторов, крупные центры обработки данных, места выхода кабелей на поверхность или центры спутниковой связи на предмет потенциальных угроз, а также последствий нарушения связи. Им можно предложить результаты оценки риска и рекомендации по лучшей защите их объектов.
- Поддерживать международные организации и их аффилированные агентства в углублении обмена информацией по надежности и безопасности Интернета на первичных линиях связи и ключевых объектах. Это сотрудничество может в конечном итоге расшириться до обмена информацией об угрозах и реагирования на них.
- Содействовать созданию правовых процессов для управления или иной формы надзора за деятельностью ответственных коммерческих провайдеров, работающих на территории страны.
- Содействовать всем правительствам в расширении доступа к Интернету имеет полезный побочный эффект увеличения спроса на надежные услуги и, таким образом, вложения инвестиций в передовые, самые эффективные технологии и управление.
- Продвигать на различных форумах предложения по внедрению государствами использования регистров маршрутизации, как передовой практики и национального стандарта. Не-регистровые и устаревшие политики маршрутизации препятствуют выявлению и анализу уязвимостей.
- Активное участвовать в международных органах по стандартизации, чтобы уменьшить поддержку идеи разделения или сегрегации Интернета.

Прекращение или ухудшение доступа к Интернету: управляемый риск

Принимая во внимание надежность Интернет-соединений в таких регионах, как континентальная часть Соединенных Штатов, между Северной Америкой и Европой, в Европе, и между всем Тихоокеанским регионом и ключевыми союзниками в Азии, можно было бы ожидать, что риск для передачи информации в этих областях будет низким. В большинстве актуальных областей, представляющих интерес, нарушение соединений увеличит задержки, но, вероятно, потребуется появление нескольких неисправностей, прежде чем увеличение задержки станет значительным. Тем не менее, непреднамеренная прокладка маршрутов нескольких ВОЛС через уязвимые туннели или вдоль мостов может привести к неприятным сюрпризам. Поскольку избыточность и безопасность являются намного менее надежными в других областях, дальнейшие исследования должны обратить пристальное внимание на конкретную организационную маршрутизацию, попытаться провести оценку с большей региональной детализацией и предложить меры по смягчению последствий. Расширение взаимодействия с бизнес-сообществом и научными кругами также может дать ценную информацию. Как отмечалось выше, также следует рассматривать безопасность энергосетей.

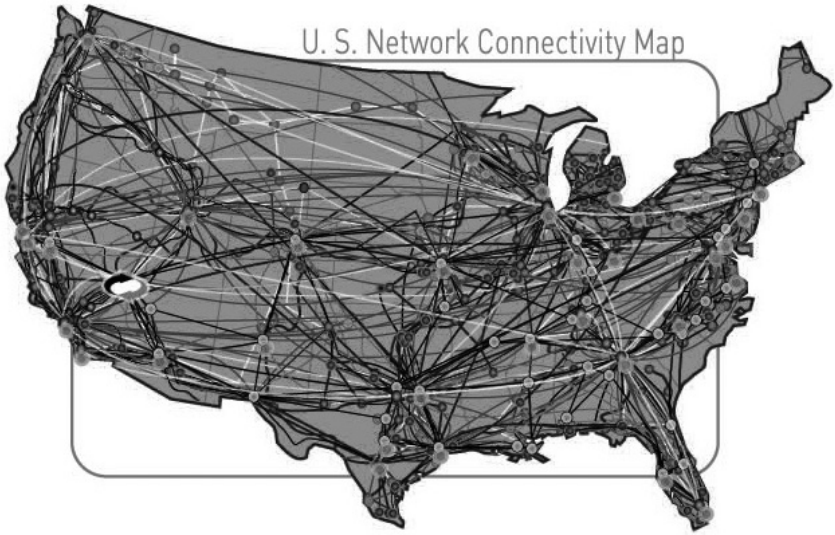


Рис. 1. Карта подключения США к Интернету

На рис. 1 показаны опорные сети и первичные подсети в США. Основными одноранговыми точками Интернет-соединения являются (с востока на запад): Нью-Йорк-Вашингтон, Чикаго-Даллас-Хьюстон, и Лос-Анджелес-Сан-Франциско[22]. Тем не менее, отображенные сети обладают значительной избыточностью, особенно на маршрутах, соединяющих Нью-Йорк, Вашингтон, Атланту, Чикаго, Южную Флориду, Канзас-Сити, Денвер, штат Калифорния и Сиэтл. Связь не зависит от одного города или одного Интернет-провайдера. Есть множество возможных путей для обхода большинства сбоев. Тем не менее, самые высокие скорости (10 Гбит сеть OC-192c/STM94) доступны только на маршруте Нью-Йорк-Вашингтон-Чикаго. По-прежнему значительные скорости в 2,5 Гбит (на сети OC48c/STM16) достигаются между побережьями через одноранговые соединения между городами[23].

Избыточность и скорость, имеющиеся на всей территории Соединенных Штатов, также присутствуют на важных трансокеанских маршрутах, например, от Большого Нью-Йорка в Великобританию, который обслуживается 6 различными подводными кабелями[24], а также на нескольких близлежащих маршрутах между Новой Англией и Францией. Аналогичные мощности имеются между США и ключевыми азиатскими союзниками и торговыми партнерами.

Это не означает, что нет никакой угрозы для устойчивости и связности информационных сетей. Проблемой может стать большая концентрация подводных кабелей, оканчивающихся вместе на европейском конце трансатлантической кабельной системы (на рис. 2), в частности, в юго-западной Великобритании (Корнуолл) и на северо-востоке Франции (Нормандская область). Слаженная и успешная операция по физическому отключению многих Интернет-узлов или соединений может привести к значительному ухудшению связи в информационных сетях частного сектора.

---

[22] Карта одноранговых соединений Интернета http://www.nthelp.com/images/interconnect.jpg

[23] Среди городов сети OC-3: Нью-Йорк-Филадельфия-Вашингтон-Атланта; Чикаго-Сент-Льюис-Даллас-Финикс; и Лос-Анджелес-Сан-Франциско-Сиэтл. См. http://www.nthelp.com/images/agis.jpg

[24] Шесть кабелей это: AC-1, AC-2, Apollo, FA-1, Tata TGN-Atlantic and TAT-14. В действительности, все эти кабели, кроме AC-2, закольцованы в Атлантике, это означает, что есть 6 отдельных трансатлантических кабельных систем Нью-Йорк-Великобритания с 11 сегментами, что обеспечивает большую пропускную способность.

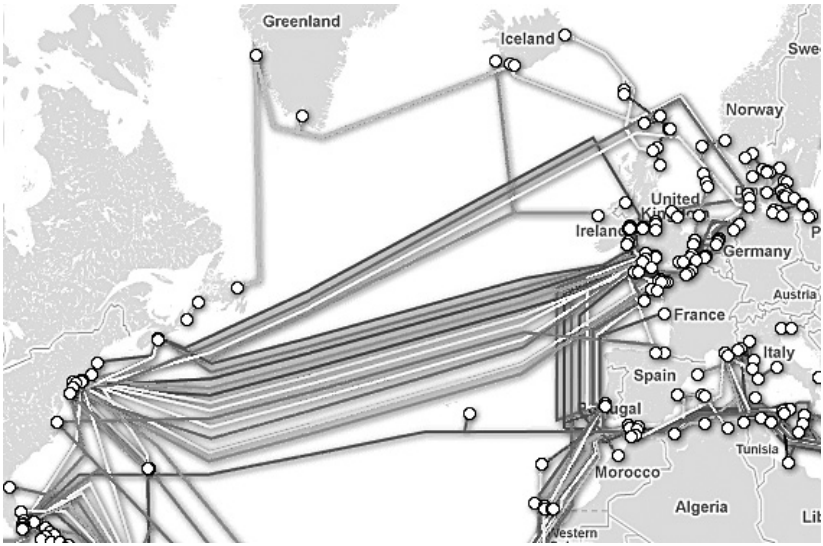


Рис. 2. Графическое изображение североатлантических кабелей

Один из сценариев, который может привести к массовому, обширному и быстрому нарушению работы Интернета, включает в себя использование электромагнитного импульса (ЭМИ). Высотный ядерный взрыв над центральной частью США будет иметь серьезные последствия, подобные эффектам геомагнитной бури высокой интенсивности, как было в 1959 году в ходе Кэррингтонского события.[25] Они могут вызвать перебои в энергоснабжении и связи на площади в тысячи квадратных миль. Механизмы повреждения отличаются: высотные ядерные взрывы создают очень короткие импульсы (так называемые импульсы E1), в то время как явления космической погоды, как правило, влияют на электрические сети посредством продолжительных событий категории E3, которые влияют на такие электрические компоненты, как трансформаторы высокого напряжения. Хотя они и маловероятны, нарушения Интернета такого рода должны быть учтены в планах действий в чрезвычайных обстоятельствах, но они выходят за рамки данного исследования.

[25] В 1959 году сочетание нескольких корональных выбросов вызвало Северное сияние на широте Панамы. Это получило название событие Кэррингтона. По оценкам, оно было на порядок интенсивнее, чем солнечная вспышка, которая вывела из строя линии электропередач в Квебеке в 1989 году. См. http://news.nationalgeographic.com/news/2011/03/110302-solar-flares-sun-storms-earth-danger-carrington-event-science/

В итоге, полное нарушение подключения к сети посредством физического нападения или чрезвычайного события маловероятно, хотя уничтожение или выведение из строя нескольких узлов или соединений может привести к частичному нарушению или ухудшению связи и обслуживания. В местах, где используется «протокол доступного кратчайшего маршрута», трафик может быть перенаправлен автоматически.[26] Тем не менее, это всё же способно привести к снижению скорости передачи данных и сбоям приложений из-за задержек или нехватки пропускной способности. Организации могут столкнуться с более высокими затратами от использования более дорогих соединений и таких альтернативных систем, как спутники. Что еще более важно, снижение качества обслуживания также может иметь серьезные последствия для времязависимых операций.

Например, серьезное нарушение Интернета во время стихийного бедствия или военного конфликта в западной части Тихого океана может иметь несколько последствий. Во-первых, коммерческие, правительственные и гуманитарные организации, в том числе военные, могут подвергнуться внезапным сбоям информационных потоков, связанных с реагированием, сбором информации, командованием, управлением и связью в регионе. Во-вторых, под угрозой может оказаться способность поддерживать продолжительные операции, если будет полностью или частично нарушена работа или скомпрометирована надежность Глобальный транспортной сети США и других систем материально-технического обеспечения. Наконец, государства должны рассмотреть возможность того, что такие действия могут привести к эскалации или перекинуться на другие информационные сети во всем мире, как военные, так и гражданские, в том числе критически важную инфраструктуру и финансовые системы. Угрозы экономической и социальной стабильности в США и других странах могут являться важными последствиями второго или третьего порядка.

---

[26] Посредством протокола доступного кратчайшего маршрута доменные сети перенаправляют трафик по кратчайшему доступному пути, следуя четкой политике маршрутизации. Протокол OSPF обычно используется внутри автономных систем таким образом, что всегда выбирается короткий/дешевый маршрут с точки зрения времени прохождения. Это не обязательно означает использование предпочтительных путей (например, тех, которыми управляют технологически надежные поставщики и которые проходят через дружественные государства) и избежание некоторых других путей (например, тех, которыми управляет недружественное государство).

Другие регионы, такие как Африка и Центральная Азия, обладают менее развитой физической инфраструктурой Интернета, но это меняется из-за быстрого развития инфраструктуры, предназначенной как для поддержания развития этих областей, так и для обеспечения транзита через них. В случае проведения операций по оказанию помощи в слаборазвитом регионе, ООН и другие учреждения, вероятно, будут в состоянии удовлетворить свои оперативные потребности путем дополнения существующей коренной инфраструктуры СВЧ-, спутниковой связью и другими возможностями, но развитие возможностей государств и повышение эффективности национальных учреждений через сочетание государственных и частных действий, вероятно, будет более эффективным и менее затратным в долгосрочной перспективе.

Может оказаться возможным воздействовать на государства или другие субъекты через помощь в наращивании Интернет-потенциала, или заставляя лиц принимающих решения сомневаться в надежности доступа в кризисных ситуациях. Однажды это может оформиться в теорию Интернет-убеждения, устрашения или сдерживания, но это другое направление исследований.

Выводы, рекомендации и дальнейший анализ

Непрерывное подключение к Интернету является необходимым для всех бизнес-операций крупных организаций, особенно для глобальных субъектов. Надежная устойчивость доступа может помочь защититься от сбоев. Единомоментных снимков сети недостаточно. Подобные организации должны иметь непрерывную ситуационную осведомленность об их текущих связях, а также системных связях вышестоящих автономных систем. Такая ситуационная осведомленность должна расширяться наружу и включать в себя понимание общей физической инфраструктуры Интернета и логической топологии, участвующих в маршрутизации трафика в сетях от пункта отправления до пункта назначения, в том числе принимать во внимание потенциальные уязвимости в логических путях, которые могут исходить из многих источников. Определение необходимого уровня качества связи требует создания стандартов, которые не могут быть полностью определены. Каждая организация может начать с улучшения устойчивости своего соединения, принимая все необходимые меры для того, чтобы все её составные структуры включали в соглашения доступа в Интернет многообразие подключений, оценку процес-

сов, организации и технологии. Отказоустойчивость также может потребовать таких новых инициатив как государственно-частное партнерство, общеправительственное участие и двусторонняя дипломатия.

Рекомендации

- Выявить автономные системы, которые имеют решающее значение для стратегической и оперативной связи организации.
- Разработать высокоточную методологию непрерывного мониторинга Интернет-зависимостей.
- Взаимодействовать с государствами и поставщиками из частного сектора в Соединенных Штатах и за рубежом, чтобы повысить связность и безопасность хотя бы критически важных сетей.
- Выработать международные инициативы, которые помогли бы государствам, в которых размещены узлы, в устранении недостатков инфраструктуры и уязвимостей.
- Проанализировать контракты с Интернет-службами и политики маршрутизации, чтобы снизить уязвимости и повысить способность быстрого перенаправления сетевого трафика, когда/где происходят сбои.
- Что касается поставщиков облачных услуг, убедиться, что резервные данные и системы не хранятся в одном облаке.
- Быть осведомленными о глобальных кризисах, которые могут потребовать перенаправления трафика компании через страны, где он не будет нарушен.

Области для дальнейшего анализа

- Изучить методологии для измерения устойчивости подключения к Интернету, чтобы определить лучшие метрики для постоянного мониторинга.
- Провести анализ связей основных субагентств, учреждений и критически важных сайтов и сравнить их устойчивость с приемлемыми показателями.
- Разработать методологию для определения автономных систем, стран и регионов, где глобальная организация имеет наибольшую уязвимость / наименьшую устойчивость.
- Объединить их в более детальном анализе устойчивости по регионам и функциям.
- Разработать систему непрерывного мониторинга отказоустойчивости, например, системы показателей, для каждой командной

структуры, учреждения, поля деятельности, критического сайта во всем мире.

- В глобальном масштабе выявить и установить профили риска для каждой критически важной точки обмена Интернет-трафиком, подводных и сухопутных кабелей, мест выхода кабелей на поверхность, крупных центров обработки данных и спутниковых станций, которые уязвимы для физического разрушения.

Charles Barry[1]

Independent Cyber Security Consult and Senior Fellow, Center for Technology & National Security Policy, National Defense University, Washington

Internet Vulnerabilities of Large Organizations: Examining Resiliency across the Autonomous Systems Layer[2]

Executive Summary

This study analyzes the resilience and vulnerabilities of large organizations' connections across the Internet. It is informed by an embedded inquiry into the dependencies of public organizations and private enterprises whose operations rely heavily on the Internet. Snapshots of both the logical topographies and physical structures of the Internet are readily available. However, logical topographies of information flows are always dynamic and visual graphics depict only a particular nanosecond of real connectivity. The physical backbone of links and nodes over which data is transmitted is less dynamic, yet it too is always changing as new structure is added and business relationships change among providers. These logical and physical maps are interdependent.

Autonomous Systems (ASes) are the primary building blocks of Internet connectivity, and they comprise the network level with the most useful information for a detailed analysis. Internet traffic paths are determined by the routing logic (policies) employed by the various AS networks involved in transiting any particular data, and by the mesh of physical links available between a given sender and its recipient. The conclusions and recommendations listed in the following Overview section of this paper are based on this AS level analysis.

Commercial services and academic research offer broad insights into the resiliency of select organizations' Internet connectivity. Some analyses show the resiliency of prominent organizations is not as robust as the best network industry entities. However, more analysis is

[1] Dr. Charles (Chuck) Barry consults in the private sector and at the National Defense University. The presentation here, including the conclusions and recommendations are his own, and do not represent any views, positions or official policies of NDU, the Department of Defense, or the U.S. Government.

[2] This paper is based a modification of unpublished research conducted between 2012–2014 at the National Defense University with Dr. Lin Wells, which itself built on earlier work by Mr. Terry Pudas and Mr. David Kay. All of us worked at the time in the Center for Technology and National Security Policy.

needed in order to define any useful vulnerability information and offer specific remedies. Rigorous research can point out the need for greater redundancy in physical connections, the advisability of customer-tailored routing policies, contractual arrangement with multiply service providers, or even international initiatives to strengthen areas of the physical infrastructure at high risk of single point failures.

From the result of such analysis two further lines of research should unfold. The first should be based on modeling and simulation to better understand the way the logical topography of the Internet responds to changes in its physical structure. This could be done using existing models and simulations as well as designing new ones. A second line of research should engage external academic and commercial enterprises already conducting analysis of transit traffic metadata to understand what other information should be considered to produce a high fidelity picture of organizational dependencies, and thus vulnerability to network disruptions. Both these initiatives would yield greater understanding of potential remedies.

Overview

Most all organizations depend on the Internet, for their very sensitive communications and information requirements as well as for the conduct of the day-to-day business operations. Connections to the Internet are thus mission critical. Reliability demands diversity of access and redundant, secure upstream topology across the entire Internet infrastructure.

The logical and physical 'maps' of the Internet are interdependent and both are highly dynamic. Routing policies employ algorithms based on conditions such as volume, shortest path to recipient, transit pricing, network availability and peering relationships. Routing policies are routinely revised by providers without notice. Physical routing choices can change abruptly based on the realities of equipment failure, latency and speed across undersea or overland cables, and congestion at Internet exchange points. The logical *un*availability of particular links and nodes is a key factor in physical routing.

The focus herein is on the AS level of the Internet. The ASes of interest are the Internet's thousands of transit service providers (ISPs). These are the on ramps as well as the nodes of the Internet, and they are where routing policies are established that govern connections within and between the many tiered networks that make up the Internet. The diversity and redundancy of these connections establish a picture of either redundant reliability or multiple vulnerabilities to

potential disruption. The physical paths of the Internet also are most manifest at the AS level. The basic building blocks are the cables and Internet exchange points (IXPs) where ISPs exchange traffic between networks. IXPs are often where major overland and undersea cables connect. Outages for any reason across these nodes and links represent the physical side of potential vulnerabilities of data during transit.

Internet traffic is monitored and mapped in detail by research centers and Internet data tracking services. Enterprises such as specialize in precise situational awareness of route congestion, equipment outages, and disruptive events like natural disasters and malware attacks. Tracking information can be tailored for commercial use, especially in the financial and energy sectors, or for government departments like ministries of foreign affairs and defense.

Maps of logical traffic flow information are depicted as either streaming graphics or snapshots, usually in milliseconds. They note traffic volume as normal or trending, and depict disruptive events that impede traffic flows. For example, Internet traffic monitoring service Renesys (since acquired by Dyn Corp) posted several time-sequence graphics depicting Internet traffic flow interruptions in Thailand during recent protests there[3].

Much of the Internet's physical infrastructure is reliable and redundant, though not always secure. An initial examination suggests that path diversity in many areas of interest might be improved (appendices 2 and 3 address vulnerabilities in undersea cables and Internet Service Providers — ISPs). However, many other factors come into play in choosing paths, including politics, business agreements, transit pricing, and router configuration.

The research reported here examines several combinations of physical infrastructures and logical topologies. A useful metric looks at the Tier level (1, 2 or 3) of immediate access providers and the number of different providers available to an organization, to produce a consolidated picture of transit diversity and resilience in the event of service disruptions. Recommendations include company policy changes and negotiating better service agreements to increase the resilience of Internet-dependent networks worldwide.

Logical topologies provide indications of potential points of vulnerability due to common factors such as high traffic volume. Logical topologies can be displayed in many ways. Nodes can be shown by

[3] See Doug Madory, *Protest Leads to Outage in Thailand*, 7:56 pm, 2 December 2013 at http://www.renesys.com/2013/12/protests-lead-outage-thailand/

content size, or their number of connections. Link thickness can reflect the normal amount of traffic carried. Maps can show the routes that packets take as a snapshot in time. These visualizations can be very interesting, even dramatic, but none that were examined offered useful insight into sustained network resilience.

The most common causes of physical disruptions are still accidental damage, equipment failure or criminal activity. Politically motivated attacks on Internet infrastructures are far less frequent, but have been increasing. Up-to-date measures of transit dependency, access redundancy and system vulnerability can help any Internet-dependent organization assess where to devote resources to improve reliability.

This research does not address all risks inherent in dependency on the Internet. The AS level does not include vulnerabilities that can be present at the sub-network level *within* each AS. The employment of routers within sub-networks (sometimes thousands of routers) may represent other single points of failure that are not visible at the AS level itself. Future research may discover other logical or physical vulnerabilities, and more work needs to be done to understand optimum connection resiliency. For very large organizations with global business interests, it may be necessary to disaggregate and prioritize the dependencies of each of their sub-entities in order to concentrate on the most critical vulnerabilities in more detail, e.g. by geographic sub-region, and prioritized sites within these areas.

Conclusions, Recommendations and Further Analysis

Robust access resiliency helps ensure continuous connectivity and guards against disruptions. Snapshots of networks at a single point-in-time or single point-of-presence are not enough. Organizations must have continuous awareness of the health of their immediate connections to the Internet as well as the systemic reliability of relevant upstream ASes. Such situational awareness has to extend beyond an organization's most common transit paths to include an understanding of the overall physical Internet infrastructure and logical topologies involved in routing traffic across networks from origin to destination, including an appreciation of potential vulnerabilities along logical paths, which may stem from many sources. Determining adequate connectivity requires standards, which are always evolving and may not be fully defined. Resiliency may also require new initiatives such as public-private partnerships, whole-of-government engagement, and bi-lateral diplomacy.

Recommendations

- Identify ASes critical to an organization's strategic and operational connectivity.
- Develop a high fidelity methodology to monitor Internet dependencies continuously.
- Work with governments and private sector providers in the United States and overseas to enhance at least the critical network connectivity and security.
- Identify international initiatives to encourage host nations to address infrastructure weaknesses and vulnerabilities.
- Examine Internet service contracts and routing policies to reduce vulnerability and enhance ability to re-route network traffic rapidly when/where disruptions occur.
- With regard to cloud service providers, ensure back up data and systems are not stored in the same cloud.
- Be aware of global crises that might require a company's traffic to be re-routed through countries where it is not subject to disruption.
- Areas for Further Analysis
- Examine methodologies for measuring the resilience of Internet connectivity to determine best of breed metrics for continuous monitoring.
- Analyze the connectivity of major sub-agencies, activities, and critical sites and compare their resilience to an acceptable requirements benchmark.
- Develop a methodology to determine the ASes, countries and regions where a global organization has the greatest vulnerability/least resiliency.
- Combine these into a more granular analysis of resilience by region and function.
- Develop a continuous resiliency monitoring system, e.g., scorecards, for each command, agency, field activity, critical site worldwide.
- Identify globally the critical Internet Exchange Points (IXPs), undersea and overland cables, cable landing points, large data centers and satellite downlinks that are vulnerable to physical disruption and establish risk profiles for each.

General

The Internet can be thought of as the global Information and Communications Technology (ICT) infrastructure — the interconnected, networked mesh of routers, switches and other purpose-designed nodes that connect computers and other information systems. The two key

components of the ICT infrastructure are its global physical architecture and its logical topology. The physical infrastructure is comprised of tangible structures and hardware located on national territory or in the undersea or space global commons. The majority of this physical infrastructure is operated by private entities. The logical topology of the Internet is determined by the routing policies (software protocols or rule sets) established by each of the administrators of the thousands of separate domains (networks) called Autonomous Systems (ASes),[4] in order to control the flow rate and path of information across and among their respective ASes.

This study concentrates on logical Internet mapping at the Autonomous Systems (AS) level based on work done by companies like Dyn (formerly Renesys) and the Network Science Research Group at the University of Louisiana — Lafayette. AS layer modeling seeks to generate a topological picture that is more detailed than the network layer, yet more aggregated than would be presented by a sub-network or router level analysis. All modeling levels have value, and each offers complementary perspectives on route topology. Ultimately, additional models, other than AS-level descriptions, would be necessary to understand Internet dependency and the diversity of access for various sub-organizations. For example, a full determination of network resilience requires analysis of downstream sub-networks and routers as well as upstream Internet exchange point (IXP) connections. This study is but a start.

The Internet is not a fixed 'network of networks.' The number and size of AS-defined networks is constantly changing. More than 45,800 ASes (as of 12 December 2013[5]) currently make up the Internet Protocol Version 4 routing system. These operate through 300 or more large Internet Exchange Points (IXPs)[6] and smaller connection nodes, and

---

[4] An Autonomous System (AS) is a set of routers under a single technical administration, using interior gateway protocols (IGP) and common metrics to determine how to route packets within the AS, and using an inter-AS border gateway protocol (BGP) to determine how to route packets to other ASs. See http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_9-1/autonomous_system_numbers.html- (March 2006) accessed 1 June 2013. The site referenced takes its definition of Autonomous Systems from Internet Exchange Task Force (IETF) document RFC 4271, edited by Rehkter, Y., Li, T., Hares, S. and entitled "A Border Gateway Protocol 4," Network Working Group/Standards Track, The Internet Society. January 2006. Page 4.

[5] See the Classless Inter-Domain Routing (CIDR) Report at http://www.cidr-report.org/as2.0/, accessed 25 September 2013

[6] This number of Internet exchange points is taken from Telegeography, Inc. See their current map at http://www.telegeography.com/telecom-resources/internet-exchange-map/index.html — accessed 12 December 2013.

over hundreds of thousands of miles of undersea and terrestrial fiber optic cables, plus space and microwave links.

ASes are often Internet Service Providers (ISP)[7] providing data transit services between one host and another. ISPs are further described as Tier 1, 2 or 3 service providers. Tier 1 ISPs are those that can reach every part of the Internet by themselves or through peering, not by purchasing transit or paying peer settlement fees to other ISPs. In the United States the top three Tier 1 providers are Level 3 Communications, Verizon Business and AT&T[8]. Tier 1 providers in other regions include NTT Communications (Japan), China Telecom, Tata (India), Deutsche Telekom AG (Germany), TeliaSonera (Europe), and Seabone (Italy)[9]. These peer-to-peer ASes typically have the greatest capacity, the most current technology and the strongest resiliency. They are often referred to informally as 'the Internet backbone'[10].

Tier 2 providers both peer with some other ISPs and buy transit rights across parts of the Internet from other, usually Tier 1, ISPs. Tier 3 ISPs only provide transit to the Internet via agreements they purchase from other ISPs. This third tier is the typical access link for individuals and small businesses. Large organizations can and should link directly to Tier 1 or Tier 2 ASes (ISPs) to increase service quality as well as reach and reliability.

The ever-changing AS composition of the Internet makes it hard to present an accurate, current map of its structure in a traditional sense. Through the use of traceroute and tracepath software, as well as other metrics, a number of commercial companies can provide minute by minute mapping, especially where superimposed on a familiar geographic reference such as a given country's borders. Providers within a country or region can be identified, with the largest service providers being relatively fixed in terms of their Tier 1 or Tier 2 status. Each ISP's market share or 'reach,' is determined by the percent of Internet Protocol (IP) addresses they service via downstream providers.

---

[7] ISPs are business ASes providing connection services to the Internet. While all ISPs are ASes, not all ASes are ISPs. For example, the DoD Network Information Center has at least four ASes (AS 721, AS2706, AS27065 and AS27066). See http://bgp.he.net/AS721 — accessed 15 December 2013.

[8] Global Internet Geography, P 10. See http://www.telegeography.com/page_attachments/products/website/research-services/global-internet-geography/0003/1871/GIG_Executive_Summary.pdf — accessed 26 May 2013.

[9] See http://drpeering.net/FAQ/Who-are-the-Tier-1-ISPs.php — accessed 3 June 2013.

[10] Tyson, Jeff, How Internet Infrastructure Works, http://computer.howstuffworks.com/internet/basics/internet-infrastructure2.htm

The physical infrastructure of the internet is made up of the AS domain networks—Tier 1, Tier 2 and Tier 3 as described above.

In large IXPs as many as 50 or 60 ASes maintain links to each other in the same building. There they can connect to multiple ASes or to undersea cable providers to pass traffic. IXPs like 60 Hudson Street and 111 Eighth Avenue in New York or 530 6th Street in Los Angeles are some of the biggest, but these types of nodes exist globally, with more than 250 being accessible for analysis via interactive maps. If transit traffic were to be interrupted at any one of these sites it would require alternate routing. In some places, e.g. the United States, alternate routing may be readily established but it could be much more difficult elsewhere, e.g., in Central Asia. In any case, some IXPs would be attractive targets should someone want to disrupt Internet traffic[11], and many are not well protected against physical attacks.

Approximately 95% of Internet traffic transits via fiber optic links, either terrestrial or undersea cable. The remaining 5% (or less) is transmitted via satellite, microwave lines, free space optics and other niche means. Fiber optic cables continue to be far more efficient than satellites in terms of operating cost, traffic capacity, signal quality, and reliability[12]. However satellites provide valuable service alternatives in contingencies operations and high priority transmissions in remote areas. Since 2011 a new generation of satellites has been improving Internet speeds and reliability at lower cost than previous satellite systems[13]. This trend is expected to gain momentum.

A third essential component of the physical infrastructure, although an indirect one, is the electrical power grid, since both nodes and links require electricity[14]. Power grids, though not dedicated exclusively to the Internet, must be considered when assessing vulnerabilities. ICT and power infrastructures go hand-in-hand and are two of the most economically critical infrastructures in any country.

---

[11] See Telegeography's Internet Exchange Map at http://www.internetexchangemap.com/ — accessed 14 July 2013

[12] http://www.fiercetelecom.com/special-reports/submarine-cable-operators-hunt-new-routes-counter-congestion-political-turm

[13] See February 2013 FCC report at http://www.fcc.gov/measuring-broadband-america/2013/February

[14] For example, one Internet node, the world's largest data center at 350 East Cermak Ave in Chicago is the city's second largest power consumer after O'Hare International Airport. Undersea cables typically require 3,000−4,000 watts of power to run the series of signal amplifiers along the cable's length.

The Internet's logical topology is determined by its routing architecture, which is based on the policies, protocols and rule sets put in place and maintained by ASs. The most prominent Internet protocol suite is a binary protocol called TCP/IP (Transmission Control Protocol/Internet Protocol). TCP/IP determines the logic of how data should be formatted, addressed, transmitted, routed and received. It is the fundamental protocol for defining the end-to-end connectivity logic across the Internet's system of networks.

Another core protocol is the Border Gateway Protocol (BGP), which ASes use in establishing their routing policies with each other's domains. TCP/IP, BGP and many other protocols define the logical Internet. ASes also use Interior Gateway Protocols (IGP) for internal routing among their IP sub-networks. Importantly, ASs have an understandable preference for routing traffic via their own sub-networks, sister networks or peer networks with which they have business routing agreements. This reality can mean taking longer routes than expected in some traffic situations. For simplicity of analysis, we will regard ASes as single entities within the routing logic of the Internet as a whole.

Among the most significant applications of the logical Internet are the operating systems of the physical links and nodes, the software utilized by the various Tiers of ISPs; and the Domain Name System (DNS) software. Like the protocols they utilize, these systems affect how traffic flows on the Internet.

The army of network administrators who set distinct routing policies for their individual AS also have considerable influence of the logical traffic flow of their customers. There are now some 72,000 allocated Autonomous System Numbers (ASNs)[15], each with a distinct set of external routing policies. These policies determine normal routing flows as well as how traffic flows will be re-directed in the event of disruptions or in emergencies. For example, ISPs can prioritize traffic of their largest clients first in terms of bandwidth availability, transit

[15] See http://www.potaroo.net/tools/asn32/. This site indicates 71,678 ASNs have been allocated to Regional Internet Registries (RIRs) as of 2 June 2013. Not all of these have been assigned to ASes (there are approximately 42,000 ASes active in the routing system). Most ASNs — more than 63,000 — are the older 16 bit ASNs. An AS may control more than one ASN. Allocation of the newer 32-bit, more flexible ASNs began in 2011. There is no mechanism for "returning" ASNs when no longer used/needed. Therefore the number should be considered an approximation of distinct routing policies employed across the Internet, though the number cited still indicates a remarkably complex mapping exercise. The website indicated is updated daily.

speeds and repairing outages. While physical maps of networks are usually available via open sources to inform users of potential risks of degraded service, administrators of private sector networks typically consider their system's actual (versus initial) routing policies, and thus much of the granularity of the Internet's logical topology, to be proprietary.

Internet Vulnerabilities

This is not a paper on cyber security, but some background on potential vulnerabilities and types of physical and logical disruptions may be useful.

Physical and logical disruptions can result from natural or man-made causes, accidental or intentional, as well as from electro-mechanical failures (including system overload). Physical disruptions can cause logical disruption and vice versa: physical damage to a network component can alter the logical flow which may affect Internet latency and bandwidth (throughput). In the run-up to military actions, cutting, jamming or otherwise disrupting (at least temporarily) key communications and information nodes can be expected. Aside from the infrastructure destruction in New York in conjunction with 9/11, terrorist attacks thus far have not caused significant disruption of Internet service (as opposed to damaging targeted facilities like the Aramco refineries in Saudi Arabia); but this has to be considered a future possibility.

Disruptions to the logical topology through malware may disrupt/degrade the physical Internet, such as a Distributed Denial of Service (DDoS) event that disrupts server capability. Point of vulnerability for the logical internet include: (1) manipulation of TCP/IP software, (2) attacks directed at ISPs and (3) attacks on the DNS itself. More information is in Appendix 3.

A key point is that a truly global strategy for reducing vulnerabilities can't primarily be technical; it must be an integrated public-private, whole of organization and government, trans-national approach mounted in parallel across people, processes, organizations and technology.

Dependency Analysis

Measuring Resilience to Internet Disruptions

Measuring an organization's resilience to Internet disruption requires an understanding of the alternative means of information trans-

fer that could be used should a particular sub-set of the Internet not be available. This is important since most of any large organization's the information, including proprietary data exchanges flows over public networks, or more accurately, is encapsulated, encrypted and tunneled[16] across the Internet infrastructure. An analysis of reliance on the Internet needs to include: (1) the criticality of a subnet, (2) the host country profile, (3) the diversity of available connections.

Criticality: What parts and regions of the Internet are most critical to the organizations and its reliance on some part of that infrastructure and logical topology constitute an unacceptable risk? It will be important to identify on which ASes the organization relies, how many of them are owned by a single provider, where the key nodes and links are, and what routing policies they have adopted. Priorities must be assigned among, for example, ASes serving command headquarters and those supporting non-front line units in remote locations. Analysts must also understand the redundancies that are available. Ultimately, similar metrics will be needed for interagency partners and allies deemed critical to national security.

Host country profiles: Organizations also needs to know the Internet infrastructure profile of the host countries in which they operate or plan to operation in the future. The number of ASNs assigned by international agreement to a country, usually to ISPs, is one recognized measure of Internet Infrastructure robustness. For example, Turkey reportedly has 290 ASNs while Azerbaijan has only 31. Other countries of note include Afghanistan with only 20 and Turkmenistan with only 2. Syria is also thought to only have two ASNs while Yemen has but one. These numbers indicate countries at risk of being disrupted significantly by natural or manmade disasters. Other countries that have little or no host nation-based Internet access include Bangladesh, Turkmenistan, Uzbekistan, Libya, North Korea and Cuba[17].

---

[16] Tunneling or 'port forwarding' is the standard technique of many Internet users to protect data. There are a host of protocols and methods, such as Microsoft's Point-to-Point Tunneling Protocol (PTPP) or secure shell (SSH protocol) tunneling, to encapsulate or encrypt payloads over untrusted networks. Tunneling sets up a vitual private network (VPN) for authorized users. See http://searchenterprisewan.techtarget.com/definition/tunneling — accessed 17 May 13

[17] The numbers cited are current as of January 2013. Autonomous System Numbers as assigned by the Internet Assigned Numbers Authority (IANA) for Border Gateway Protocol (BGP) routing use (BGP is the core protocol within the TCP/IP protocol). ASes in a country are usually ISPs and the number of ASNs allocated within a country is one measure of Internet infrastructure robustness. See http://www.renesys.com/tech/presentations/pdf/menog12-cowie.pdf — accessed 19 May 13.

Transit Diversity: How much diversity does any particular sub-organizational entity have in reaching the Internet's top level ISPs? When an organization's primary provider, node or link is degraded, are alternate providers and conduits already connected, ready and able to maintain presence seamlessly? This is a deeper question than just the number of ASes directly servicing each critical network of any multi-national corporation or global organization. The answer has to include analysis of upstream providers and the routing architecture all the way up to the Internet backbone in order to see if multiple ASes converge at some single point of vulnerability. ISP business relationships are constantly in flux and with them the routing architectures of the affected ASes. An effective analytical process has to include continuous communication with service providers and periodic routing updates.

Resilience is a function of transit diversity that is achieved not only by using multiple direct AS providers, but also by ensuring multiple paths among upstream indirect providers all the way to the Internet backbone. In addition to assessing direct and indirect provider relationships for each of its principal subordinate entities, every global organizational has to be aware of the business relationships of their Internet service providers. Do some or all providers pass through the same parent AS? Are critical ASes vulnerable to de-peering actions that could make it difficult for them to connect with customers or collaborators? If so, an organization-wide disruption could generate perturbations across all ASes servicing one or many connections.

A recent Dyn/Renesys analysis looked at routing data at the AS level to assess direct and indirect diversity by studying relationships among providers. They then scored organizations on their degree of transit diversity, from none (a score of zero) to rich diversity with no single points of failure (a score of 100). The scatter plot in Chart A below represents scores for tens of thousands of organizations with Internet presence, grouped by the number of ASes employed (vertical axis). Notably, the United States Department of Defense (DoD), just one of many organizations in the analysis, scored low at 34, potentially indicating significant potential for improving the transit diversity of its Internet presence[18]. The low DoD score likely reflects a large, dispersed organization with a multitude of individual, locally contracted transit providers. In addition, a DoD-wide scoring result at any point on the scale does not tell us much as there is no indication of where transit diversity is low and where it might be sufficient. Are major commands

[18] See http://www.renesys.com/2009/05/keeping-score/ — accessed 31 May 2013

vulnerable to disruption? There is no breakdown among the multitude of subordinate commands or agencies dealing in such functions as logistics or personnel. The Renesys algorithms are proprietary, but more detailed analysis of the data set is possible and would likely be useful.

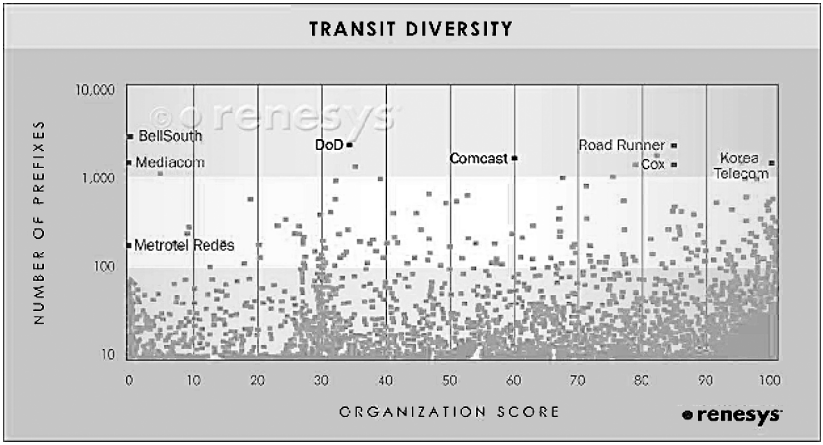


Chart A. A Renesys Transit Diversity scorecard

A Dual Direct — Indirect Dependency: The Electric Power Grid

Internet dependence related to electric power grids is both direct and indirect. Most organizations with critical networks maintain back-up or emergency power supplies such as generators to compensate for power outages, however some are investigating dual-sourced electrical feeds for key installations. This is important since emergency fuel can run out or back-up components fail. Most all critical Internet infrastructures are operated by the private sector. Private sector infrastructure continuity of operations (COOP) mechanisms vary in quality, but most do have backup power capacity, albeit for limited periods. Thus, widespread, long duration power outages that affect multiple service providers could degrade Internet performance for many users. Disruptions of power and Internet service also may make it impossible for consumers to pay for critical commodities like fuel and medicine, with potential consequences for social stability[19].

[19] The inability of customers to pay for gasoline with credit cards after Hurricane Sandy is one example. A 2011 NDU study of severe space weather events found that prolonged power outages over wide areas would generate particular concern among the public over pharmaceutical distribution.

In addition to physical and logical vulnerabilities that could hinder an organization's ability to use the Internet globally, providers abroad may not be paying enough attention to infrastructure modernization or security. A related concern is that unrest in countries with weak governance or unfriendly national governments could block, or distort, Internet transits within their borders through legal maneuvers or other actions.

Some states regulate Internet content and control telecommunications through government-owned companies, or own the physical infrastructure required to connect to the Internet. Authoritative regimes have also acted to suppress Internet access when a crisis arises. During the January 2011 protests in Egypt the government invoked a national security provision in its telecommunications law to direct foreign wireless carriers to disable access to mobile networks. Most did initially, though later some restored limited services[20]. The gambit had little or no effect on the revolt as protesters rallied to work around the restrictions[21]. However, the action demonstrated the degree to which some states will seek to limit access to unfiltered information and the Internet.

It should be assumed that in authoritarian states, the private (for profit) sector, the citizenry, and third parties (international Internet operators and users) will have little or no recourse to legal appeal or regulatory against state actions to interfere with the Internet. At the same time, poor physical or cyber security also could open holes that could disable or degrade Internet connectivity based on non-attributable actions from almost any geographical area.

Considerations for diplomatic, legal or commercial engagement to reduce vulnerabilities

Diplomatic, legal, or commercial engagement, at various levels, may be able to reduce vulnerabilities and broaden the redundancy of

---

[20] See http://latimesblogs.latimes.com/babylonbeyond/2011/01/egypt-foreign-telecomms-stepping-in-to-connect-protesters-to-internet.html. France Telecom and Vodafone Group were two that restored service after a few days. Others relied on land lines and old dial up services to circumvent the wireless interruption.

[21] See http://www.aljazeera.com/news/middleeast/2011/01/201112515334871490.html, accessed 26 May 2013. Over the weekend of January 30–31 2011 collaboration between Google, Twitter and a voice messaging service just acquired by Google called SayNow led to an announcement of a toll free international phone service called "speak2tweet" where Egyptian users could leave a twitter message for others. The success of this effort in circumventing efforts to control social media led to a duplicate speak2tweet service in Syria, launched in December 2012 as that government threatened to disrupt public access to social media services and the Internet.

the Internet abroad. The most important step is to convince governments to treat the security and reliability of information and communications, and their related infrastructures (ICT), with a much higher priority than they now are. These capabilities are helping to determine winners and losers in economies, affecting international relations and changing the way our children think. Yet they rarely are treated as either essential services or critical infrastructures in interagency priorities. These are issues for business and government leaders and policy makers, not just cyberspace technicians. Some opportunities are:

- Encourage countries that lack sufficient redundancy within their borders to increase routing diversification of at least their main conduits. Network resiliency could be added to the agenda of transit fee negotiations.
- Engage on plans for new or upgraded fiber optic cables overland or undersea, often backed by consortia of multinational companies and the countries to be served. Multinational consortia can be encouraged to include protective measures in their design, such as burying undersea cables, hardening overland connection points, installing the latest monitoring and investing in robust maintenance capacity.
- Appraise countries who host telco/carrier hotels, large data centers, cable landing points or satellite downlinks of potential threats as well as the ramifications of disruption. They might be offered risk assessment evaluations and recommendations to protect their sites better.
- Encourage international organizations and their affiliated agencies to deepen information sharing on the reliability and security of the Internet across primary links and at key sites. This cooperation might eventually extend to sharing threat information and response actions.
- Promote the establishment of legal processes to govern, or otherwise oversee, the actions of responsible commercial providers operating on national territory.
- Encourage all governments to increase access to the Internet has the spin-off effect of increasing demand for reliable services and thus investment in the latest, most capable technologies and management.
- Advocate in various fora that nations foster use of routing registries as a best business practice and national standard. Non-registry and out-of-date routing policies hamper trace back and analysis of vulnerabilities.
- Engage aggressively in international standards bodies to reduce support for Internet disruption or segregation.

Denied or Degraded Internet Access: A Manageable Risk

Given the robust Internet connections in regions such as the continental United States, between North America and Europe, inside Europe, and across the Pacific to key Asian allies, one would expect that the risk to transmissions in these areas would be low. In most current areas of interest failures of links would add latency, but it probably would take multiple failures before the increased latency becomes significant. Nevertheless, it is possible that the unintended routing of multiple fiber optic links through vulnerable tunnels or along bridges could lead to unpleasant surprises. Since redundancy and security are much less robust in other areas, subsequent research should look at particular organizational routing in more detail, attempt to understand the scoring with more regional granularity, and suggest mitigation measures. More work should be done with the business community and academic research also may yield valuable insights. Power grid security also needs to be considered as noted above.

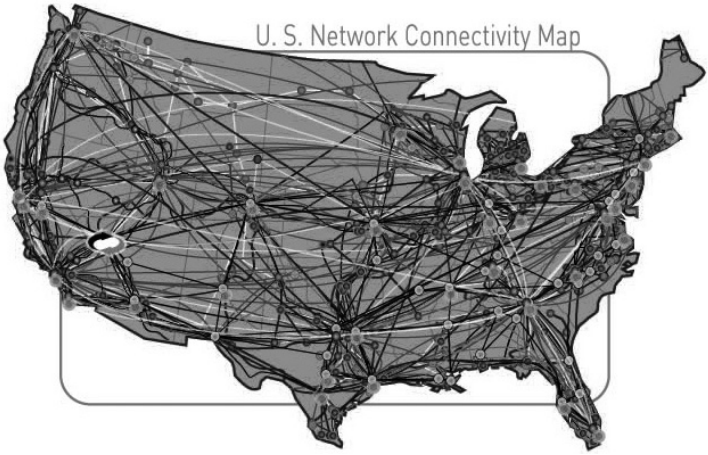


Figure 1. U.S. Internet Connectivity Map

Figure 1 depicts the U.S. Internet backbone and primary subnetworks. Major Internet peer-to-peer interconnect points are (East to West): New York-Washington, Chicago-Dallas-Houston, and Los Angeles-San Francisco[22]. However, the networks shown have heavy redundancy, especially on routes connecting New York, Washington, Atlanta, Chicago, South Florida, Kansas City, Denver, California and

[22] Internet Peer-to-Peer Interconnect map at http://www.nthelp.com/images/interconnect.jpg — accessed 26 May 2013.

Seattle. Connectivity is not dependent on one city or one network provider. Rather there are many possible paths to reroute around most disruptions. However, the highest speeds (the 10 Gbps OC-192c/STM94 Network) are available only from New York-Washington-Chicago. Still impressive speeds of 2.5 Gbps (on the OC48c/STM16 Network) are found coast to coast among peer-to-peer cities[23].

The redundancy and speeds found across the United States also are present on important transoceanic routes, such as from greater New York to the United Kingdom, which is served by 6 different undersea cables[24] plus several nearby routes to and from New England and France. Similar capacity is present between the U.S. and key Asian allies and trading partners.

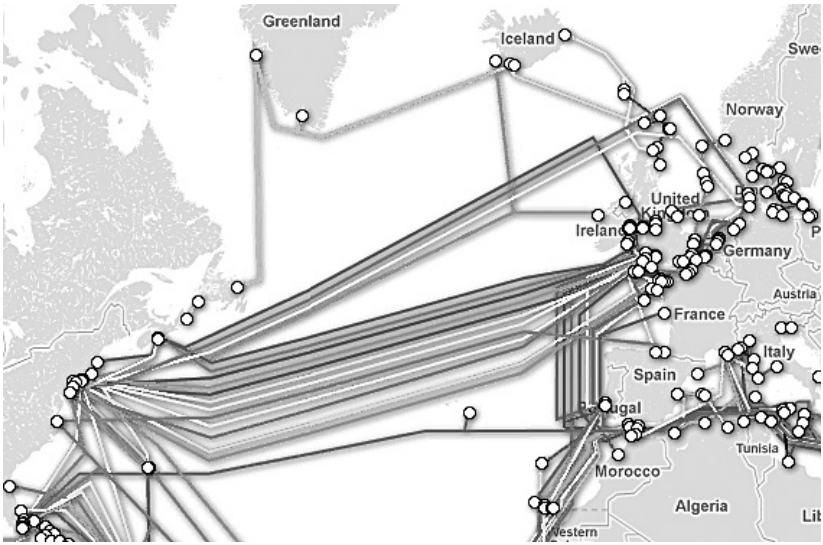


Figure 2. North Atlantic Cable Graphic

This does not mean that there is no threat to information networks' resilience and connectivity. A case in point can be seen in the greater concentration of undersea cables terminating together on the Euro-

[23] The OC-3 Network cities include New York-Philadelphia-Washington-Atlanta; Chicago-St. Louis-Dallas-Phoenix; and Los Angeles-San Francisco-Seattle. See http://www.nthelp.com/images/agis.jpg

[24] The 6 cables are AC-1, AC-2, Apollo, FA-1, Tata TGN-Atlantic and TAT-14. In fact, all of these cables, except AC-2 run in loops across the Atlantic, meaning that there are 6 distinct NY-UK transatlantic cable systems with 11 segments allowing for even greater traffic.

pean end of the transatlantic cable system in Figure 2, particularly in southwestern United Kingdom (Cornwall) and northeastern France (Normandy region). A well-coordinated and successful operation to disable many Internet nodes or pathways physically could result in major degradation of private sector information networks.

One scenario which could lead to a massive, wide area and rapid degradation of the Internet involves electromagnetic pulse (EMP). A high altitude nuclear burst over the central United States would have significant consequences, as would a high intensity geomagnetic storm, such as the 1859 Carrington Event[25]. Either could cut electrical power and communications connectivity over thousands of square miles. The damage mechanisms are different: High altitude nuclear bursts generate very short duration pulses (so-called E1 pulses), while space weather events typically affect power grids through long duration E3 events that affect electrical components such as high voltage transformers. Although unlikely, these kind of Internet interruptions need to be considered in contingency plans, but they're outside the scope of this study.

In sum, total denial of network connectivity through physical attacks or accident is unlikely, although a partial denial or degradation of connectivity and service could result from the disruption or destruction of several nodes or pathways. Traffic could be re-routed automatically where the "open shortest path first" protocol is employed[26]. However, this still could result in delayed data transmission and application failure due to latency or a bandwidth shortage. Organizations could see higher costs from the use of more expensive bandwidth and alternative systems, such as satellites. More importantly the degraded service also could have serious impacts on time-sensitive operations.

For example, a serious Internet disruption during a natural disaster or military conflict in the Western Pacific could have multiple effects.

---

[25] In 1859 a combination of multiple Coronal Mass Ejections (CME) caused the Northern Lights to be visible as far south as Panama. This was known as the Carrington Event. It has been estimated that this event was as much as ten times more intense than the solar storm the dropped the Quebec power grid in 1989. See http://news.nationalgeographic.com/news/2011/03/110302-solar-flares-sun-storms-earth-danger-carrington-event-science/ — accessed 15 December 2013

[26] Through "open shortest path first" or OSPF, domain networks re-route traffic through the shortest available path by following a distinct routing policy. The OSPF protocol is usually employed internal to an AS and automated such that the shortest/lowest cost route in terms of transit time is always chosen. It would not necessarily use preferred pathways (e.g., those run by technologically reliable vendors and transiting friendly states) and avoid certain other pathways (such as those operated by an unfriendly power).

First, commercial, government and humanitarian relief organizations, including militaries could suffer immediate disruptions in information flows related to response operations, information gathering, and command, control and communications across the region. Second, the ability to sustain prolonged operations might be jeopardized if the U.S. Global Transportation Network and other logistical support systems were disrupted/degraded or thought to be unreliable. Finally, governments would have to consider the possibility that such disruptions could escalate or widen to other information networks, both military and civilian worldwide, to include critical infrastructure and financial systems. Threats to economic and social stability in the U.S. and elsewhere may be crucial second or third order effects.

Other regions, such as Africa and Central Asia have less-developed physical Internet infrastructure, but this is changing due to rapid infrastructure development intended both to support these areas and transit through them. In the event of relief operations in a less-developed region, the UN and other agencies probably would be able to meet operational needs by augmenting existing indigenous infrastructure with microwave, satellite and other capabilities, but the development of partnering nation capacity, and effective host nation institutions, through a mix of public and private means is likely to be more effective and less costly in the long run.

It may be possible to exert leverage on states, or other actors, by supporting the build-up of an Internet capability, or causing doubts in decision makers' minds about their ability to count on continued access in a crisis. This might one day be formed into a theory of Internet-based suasion, dissuasion, or deterrence, but that is for a different line of research.

Conclusions, Recommendations and Further Analysis

Continuous connectivity across the Internet is essential to all business operations of large organizations, especially global entities. Robust access resiliency can help guard against disruptions. Single point snapshots aren't enough. Such organizations must have continuous situational awareness of their immediate connectivity as well as the systemic connections of upstream ASes. Such situational awareness has to extend externally to include an understanding of the overall physical Internet infrastructure and logical topologies involved in routing traffic across networks from origin to destination, including an appreciation of potential vulnerabilities along logical paths, which may stem from many sources. Determining adequate connectivity requires establishing

standards, which may not be fully defined. Each organization can begin to improve its connection resilience by ensuring all its components incorporate diversity into Internet access agreements, assessing processes, organizations and technology. Resiliency may also require new initiatives such as public-private partnerships, whole-of-government engagement, and bi-lateral diplomacy.

Recommendations

- Identify ASes critical to an organization's strategic and operational connectivity.
- Develop a high fidelity methodology to monitor Internet dependencies continuously.
- Work with governments and private sector providers in the United States and overseas to enhance at least the critical network connectivity and security.
- Identify international initiatives to encourage host nations to address infrastructure weaknesses and vulnerabilities.
- Examine Internet service contracts and routing policies to reduce vulnerability and enhance ability to re-route network traffic rapidly when/where disruptions occur.
- With regard to Cloud service providers, ensure back up data and systems are not stored in the same cloud.

Areas for Further Analysis

- Examine methodologies for measuring the resilience of Internet connectivity to determine best of breed metrics for continuous monitoring.
- Analyze the connectivity of major sub-agencies, activities, and critical sites and compare their resilience to an acceptable requirements benchmark.
- Develop a methodology to determine the ASes, countries and regions where a global organization has the greatest vulnerability/least resiliency.
- Combine these into a more granular analysis of resilience by region and function.
- Develop a continuous resiliency monitoring system, e.g., scorecards, for each command, agency, field activity, critical site worldwide.
- Identify globally the critical Internet Exchange Points (IXPs), undersea and overland cables, cable landing points, large data centers and satellite downlinks that are vulnerable to physical disruption and establish risk profiles for each.

Джон Э.Сэвидж
Университет Брауна (США)

Брюс В.Макконнелл
Институт Восток-Запад (США)

Изучение управления Интернетом с участием всех заинтересованных сторон[1]

Краткое содержание

Интерес к вопросу управления Интернетом подогревается вниманием средств массовой информации к киберпреступности, глобальной слежке, коммерческому шпионажу, кибератакам и угрозам критически важным национальным инфраструктурам. Многие государства решили, что им требуется больше контроля над Интернет-технологиями и основополагающими принципами. Другие страны, подчеркивая положительные аспекты этих технологий, утверждают, что должны по-прежнему преобладать традиционные системы управления Интернетом, которые они называют «многостороннее участие», и с которыми они связывают успех Интернета.

В этой статье мы рассмотрим подход с участием всех заинтересованных сторон в историческом контексте, как он на протяжении многих десятилетий применялся в других областях. Затем, мы рассмотрим многостороннее управление Интернетом.

Даётся три рекомендации. Во-первых, мы предлагаем упростить управление Интернетом путем расчленения его на вопросы, которые могут быть решены в рамках существующих международных учреждений, и на все остальные, среди которых — вопросы присвоения имен, маршрутизации, безопасности и стандартизации. Эти вопросы, прежде всего, являются техническими, но в них есть и политическое измерение. Во-вторых, органам, занимающимся техническими или связанными вопросами (таким, как Интернет-корпорация по присвоению имен и номеров (ICANN), мы рекомендуем добавить надзорный уровень с многосторонним участием, который может принимать или отклонять позицию этих органов, но не изменять её. В-третьих, работа су-

[1] Это сокращенная версия более обширной статьи, опубликованной Институтом Восток-Запад

ществующих международных организаций, занимающихся решением других вопросов, должна быть изменена таким образом, чтобы получать отклик от Интернет-сообщества посредством многосторонних консультативных процессов. С учетом этих изменений управление Интернетом может стать более всеобъемлющим и управляемым, при этом сохраняя свои самые ценные качества.

Введение

Интерес к вопросу управления Интернетом неуклонно возрастает с момента создания Интернет-корпорации по присвоению имен и номеров (ICANN) в 1998 году, и в настоящее время обсуждается на многих международных форумах. Всемирная встреча на высшем уровне по вопросам информационного общества (ВВУИО), состоявшаяся в 2003 и 2005 году, была знаковым событием. В пункте 24 Тунисской программы ВВУИО 2005 года, содержится следующее рабочее определение управления Интернетом.

Рабочее определение управления использованием Интернет означает разработку и применение правительствами, частным сектором и гражданским обществом в рамках исполнения ими своих соответствующих ролей общих принципов, норм, правил, процедур принятия решений и программ, которые формируют условия для развития и использования Интернет.

Генеральный секретарь ООН создал Форум по управлению Интернетом как ответвление ВВУИО, и он ежегодно проводится с 2006 года. Форум является важной площадкой, где тысячи участников обмениваются идеями по вопросам управления Интернетом, но не обладают правом давать рекомендации.

В 2013 году ведущие организации, отвечающие за глобальную координацию технической инфраструктуры Интернета, встретились в Монтевидео (Акплоган и др., 2013 г.) и «определили необходимость постоянной работы над сложностями, возникающими в отношении управления Интернетом, и согласились активизировать работу в рамках всего сообщества для обеспечения развития глобального сотрудничества в сфере Интернета с участием многих сторон».

После этой встречи, в апреле 2014 года в Бразилии был проведен «NETmundial»: всемирная встреча различных заинтересованных сторон по вопросу будущего управления Интернетом (ICANNWiki, 2014 год). Результатом этого мероприятия стал набор принципов и дорожная карта развития Интернета, которые

были одобрены большинством участников, но не Китаем, Индией или Россией. Они предпочитают «государство-центричный подход к управлению Интернетом под эгидой ООН» (Корвин, 2014 год).

Один из принципов управления Интернетом, выработанных в ходе процесса NETmundial, гласит «управление Интернетом должно быть основано на демократических процессах с участием всех заинтересованных сторон и должно обеспечить реальное и подотчетное участие всех заинтересованных сторон, включая правительства, частный сектор, гражданское общество, техническое сообщество, научное сообщество и пользователей».

В настоящее время, модель участия всех заинтересованных сторон широко освещается как предпочтительная модель управления Интернетом. Белый дом одобрил её в Международной стратегии для киберпространства 2011 года, а обе палаты Конгресса США в конце 2012 года. ICANN характеризует себя как организацию с участием всех заинтересованных сторон (ICANNWiki, 2014 год), а Международный союз электросвязи (МСЭ) в документе Всемирного форума по политике в области электросвязи 2013 года (ВФПЭ) заявил, что «члены МСЭ в своих полномочных резолюциях признают основанную на принципах ВВУИО модель управления с участием всех заинтересованных сторон в качестве основы для глобального управления Интернетом» («Supporting Multi-stakeholderism in Internet Governance,» 2013).

Учитывая то, какую известность получил вопрос управления Интернетом с участием всех заинтересованных сторон, важно понять, что означает это понятие, изучить его сильные и слабые стороны, и понять, как лучше реализовать его. Для мирового сообщества будет неблагоразумно принять эту форму управления таким важным глобальным ресурсом, как Интернет, в отсутствие полного понимания этих вопросов.

Инициативы по управлению с участием всех заинтересованных сторон являются привлекательными, поскольку они могут обеспечить альтернативу между крайностями политики невмешательства и государственного регулирования, развивая сотрудничество между неправительственными организациями и корпорациями в форме саморегулирования.

К сожалению, нет общепринятого определения управления с участием всех заинтересованных сторон. Концепция начала использоваться как средство для развития сотрудничества в решении таких социальных проблем как возобновляемость природных ресурсов и защита трудящихся в развивающихся странах.

Далее, мы рассмотрим краткую историю управления Интернетом; общие исследования инициатив с участием всех заинтересованных сторон; и изучим текущее состояние проблем управления Интернетом. Мы также подробно рассмотрим вопросы управления Интернетом и дадим пояснения по нашему предлагаемому упрощению управления Интернетом через распределение вопросов среди существующих международных органов. Для технических вопросов мы рекомендуем, если у существующего органа есть политический уровень (как в ICANN), оградить технические решения от изменений на политическом уровне. Для нетехнических вопросов управления Интернетом мы рекомендуем добавление компонентов участия всех заинтересованных сторон в международные органы, ответственные за вопросы управления Интернетом.

Краткая история управления Интернетом

Истоки Интернета, как научно-исследовательского проекта DARPA, хорошо известны. Популярность ARPANET и его преемника, сети Интернет, привела к его распространению в мире. Появилась Инженерная рабочая группа Интернета (Internet Engineering Task Force (IETF), как площадка для исследователей для обсуждения и продвижения новых сетевых технологий без участия руководителей программ из DARPA. Возник Консорциум мировой сети (World-Wide Web Consortium (W3C), чтобы выполнять аналогичную роль для веб-технологий. Следует отметить, что для реального участия в работе этих органов требуются глубокие знания соответствующих технологий.

IETF создал неформальную, но хорошо выстроенную систему для обеспечения своей работы. Его рекомендации отражены в тысячах документов, называемых Запросами для обсуждения (Request for Comments (RFCs). RFC 7154 содержит кодекс поведения Инженерной рабочей группы Интернета, а именно, что участники должны оказывать уважение и быть вежливыми друг к другу, вести объективные дискуссии, быть готовыми внести свой вклад и работать вместе для выработки решений для глобальной сети Интернет. Запрос для обсуждения де-факто становится стандартом, если он широко принят многими поставщиками.

Открытая, инклюзивная, прозрачная и не-запретительная философия, которая лежала в основе создания Интернет-технологий, способствовала участию инженеров в их развитии, а пользователей — в создании веб-контента.

Структура управления Интернетом сложна и имеет много участников. Примечательно то, что она надежно обслуживает население, которое по оценкам насчитывает более трех миллиардов пользователей. В свете этого, попытки заменить важные части нынешней системы управления должны делаться с большой осторожностью. Другой вывод состоит в том, что Интернет-пространство, скорее всего, слишком сложно, чтобы находиться в ведении одной организации. Оно хорошо функционирует благодаря опыту, распределенному среди многих участников.

Что представляет собой управление Интернетом с участием всех заинтересованных сторон?

Термин управление с участием всех заинтересованных сторон используется для Интернета с 2004 года. Маркус Куммер определяет его как средство «политического диалога, в котором все заинтересованные стороны участвуют на равных» в рамках процесса, который прозрачен и открыт для всех (Куммер, 2013). «В то время как участие всех заинтересованных сторон в Рабочей группе по управлению Интернетом и Форуме по управлению Интернетом означало и означает, что все заинтересованные стороны принимают участие на равных, также понятно, что в большинстве организаций, как межправительственных, так и других, существуют определенные структуры для осуществления процессов принятия решений» (Куммер, 2013).

По словам Лоуренса Е Стриклинга, руководителя Национального управления по телекоммуникациям и информации (NTIA) Министерства торговли США, «процесс с участием всех заинтересованных сторон... включает в себя полное участие всех заинтересованных сторон на основе консенсусной выработки решений и работу в открытом, прозрачном и подотчетном виде».

В этих определениях не указаны принципы создания организаций с участием всех заинтересованных сторон кроме того, что они должны быть открытыми, прозрачными и инклюзивными. Они не определяют, как должны идти процессы, помимо того, что «заинтересованные лица участвуют на равных», и что решения должны приниматься «на основе консенсуса». Указанные упущения ставят под сомнение, создают ли эти описания процессов с участием всех заинтересованных сторон достаточное основание, на котором можно выстроить глобальную систему управления Интернетом. Рассмотрим инициативы с участием всех заинтересованных сторон в иных областях.

Исследование общих примеров управления с участием всех заинтересованных сторон

Мину Хеммати (Хеммати, 2002) говорит, что процессы с участием всех заинтересованных сторон использовались в течение многих десятилетий для решения проблем в различных областях, включая биотехнологии, корпоративное поведение, энергетику, гендерное неравенство, туризм, трудовые отношения, горнодобывающую промышленность и устойчивое развитие. Она отмечает, что процессы с участием всех заинтересованных сторон доносят информацию до лиц, принимающих решения, обеспечивают поддержку решений, ищут пути решения проблем и побуждают заинтересованные стороны брать на себя ответственность в решении вопросов. Этот подход был эффективен во многих социальных, политических, экономических и технических условиях, особенно когда возникающие проблемы являются качественно новыми, быстро изменяющимися и обременены важными социальными и культурными измерениями. В этих условиях правительства, как правило, действуют медленно. Через взаимодействие в рамках процесса с участием всех заинтересованных сторон можно быстро получить доступ к кадрам, необходимым для решения сложных новых проблем.

После изучения 20 различных процессов с участием всех заинтересованных сторон, Хеммати (Хеммати, 2002) определяет их как «*процессы, которые направлены на объединение всех основных заинтересованных сторон* в новой форме общения, в поиске (и, возможно, принятии) решений по конкретному вопросу. Они также основаны на признании важности достижения равенства, справедливости и подотчетности в процессе общения и обмена взглядами между заинтересованными сторонами. Они строятся на демократических принципах прозрачности и участия и нацелены на развитие партнерских связей и укрепление взаимодействия между заинтересованными сторонами». Она также говорит, что «процессы с участием всех заинтересованных сторон охватывают широкий спектр структур и уровней участия. Они могут представлять собой обсуждение политики или расширяться и включать в себя поиск консенсуса, принятие и реализацию практических решений... Таким образом, процессы с участием всех заинтересованных сторон бывают разными по форме».

Она предупреждает, что «процессы с участием всех заинтересованных сторон не являются универсальным инструментом

или решением всех вопросов, проблем и ситуаций. Они больше похожи на новый тип взаимодействия в системе выработки решений и структурах и процессах управления. Они подходят для тех ситуаций, когда возможен диалог, и где уместно и возможно прислушаться, согласовать интересы и интегрировать мнения в общие стратегии решения.» Цитируя Кадер Асмал в вопросе выбора между обсуждением и прямыми действиями, она предупреждает нас, «Зачастую процесс становится запутанной, рыхлой, раздражающей и разваливающейся какофонией. Как и плюралистическая демократия, он является самой худшей формой поиска консенсуса за исключением всех остальных».

Хеммати (Хеммати, 2002) отмечает, что создание процессов с участием всех заинтересованных сторон требует принятия решений, касающихся Секретариата, физической поддержки организации, финансирования, отчетности и документации, связей с общественностью и вопроса наличия и способа связи с официальным процессом принятия решений. Более конкретно она отмечает, что необходимы решения по широкому спектру вопросов, в том числе:

a. определение проблем, которые предстоит решать;

b. принятие решения о том, какие заинтересованные стороны должны быть приглашены;

c. проводится ли участие только по приглашению, открыто для всех или для ограниченного числа представителей от каждой заинтересованной стороны;

d. установление сроков для осуществления действий;

e. подготовка совещаний;

f. связь между заинтересованными сторонами, например, через онлайн, местные, региональные или более широкие совещания;

g. устранение неравенства в возможностях между заинтересованными сторонами вследствие разного уровня опыта или доступа к средствам;

h. необходимость и/или способ вынесения рекомендаций и/или решений (необходим ли консенсус?);

i. условия, при которых прекращается деятельность процесса с участием всех заинтересованных сторон.

Вальехо и др. (Вальехо и Хаузельманн, 2004) отмечают, что возникли многие неправительственные организации и бизнес-инициативы, которые занимаются добровольным негосударственным «нормотворчеством, сертификацией и маркировкой, коллективными соглашениями для формирования политики в

конкретных областях, мерами по управлению цепями поставок или... выработкой правил поведения». В то время как их анализ инициатив с участием всех заинтересованных сторон является не таким всеобъемлющим, как у Хеммати, они отмечают, что жизнеспособность подобных инициатив в значительной степени зависит от их легитимности и эффективности. Они приводят определение легитимности 1955 года по Зухманну как «обобщенное восприятие или предположение, что действия субъекта желательны, верны и приемлемы в некоторой социально выстроенной системе норм, ценностей, убеждений и определений».

В продуманном и глубоком исследовании 2012 года, ван Хёйстэ (Хёйстэ, 2012) предлагает стратегическое руководство для общественных организаций, которые намерены участвовать в инициативах с участием всех заинтересованных сторон, призванных помочь корпорациям в экологически рациональном использовании природных ресурсов. Она предлагает рекомендации в отношении многих аспектов организации инициатив с участием многих заинтересованных сторон. В своём исследовании она заявляет, что необходимо понимать возможную роль правительств, так как «инициативы с участием многих заинтересованных сторон по самой своей природе являются гражданскими инструментами (или, с точки зрения бизнеса, саморегуляцией)». «Роль государственных органов может заключаться в поощрении, созыве участников, содействии или финансировании инициатив с участием всех заинтересованных сторон, но они, скорее всего, не станут обсуждать стандарты с общественными организациями или представителями бизнеса». Она также говорит, что «в долгосрочной перспективе, инициативы с участием всех заинтересованных сторон могут использоваться как экспериментальные механизмы, которые начинаются в виде добровольных инициатив, но постепенно трансформируются в государственную политику и регулирование». Далее мы переходим к анализу управления Интернетом.

Сфера управления Интернетом

Большинство предложений по управлению Интернетом с участием всех заинтересованных сторон включает в себя слишком много тем. Это видно на примере Форума по управлению Интернетом, прошедшего в 2014 году в Стамбуле. Обсуждались вопросы доступа к Интернету, свобода выражения мнений, безопасность детей, конфиденциальность, экономика открытого

Интернета, развертывание IPv6, доступность Форума для лиц с ограниченными возможностями, «право быть забытым», гендерные вопросы, изменение климата, Интернет вещей, права человека, общественный доступ к библиотекам, мобильный Интернет и безопасность, надежность и устойчивость сети Интернет. Чтобы решить проблему управления Интернетом, её необходимо упростить.

В своем предисловии (к Капур, 2005), Винт Серф обращает внимание на эту проблему: «За некоторыми исключениями, большинство вопросов государственной политики, связанных с Интернетом, лежат вне компетенции ICANN и могут и должны быть решены в других местах. Например, проблема спама, в том числе в системах обмена мгновенными сообщениями и интернет-телефонии,.. может быть успешно решена только с помощью правовых средств, хотя есть некоторые технические меры для фильтрации нежелательных сообщений, которые могут быть предприняты интернет-провайдерами (ISP) и конечными пользователями. Аналогично, такие виды мошенничества как «фишинг» и «фарминг» лучше всего решать с помощью правовых средств. Проблема защиты интеллектуальной собственности отчасти может быть решена через Всемирную организацию интеллектуальной собственности (ВОИС) и коммерческие споры в рамках Всемирной торговой организации (ВТО) или с помощью альтернативных методов разрешения споров, таких, как посредничество и арбитраж». Ниже мы рассмотрим разделение управления Интернетом на отдельные темы. Но перед этим мы обратим внимание на проблемы существующего состояния управления Интернетом.

Современное состояние управления Интернетом

В управлении с участием всех заинтересованных сторон задействованы стейкхолдеры, которые, опираясь на свой опыт и энтузиазм, создают новые технологии или веб-контент. Этот процесс не только более гибкий, чем действия государств, он также способствовал внедрению инноваций и стимулированию экономики. Тем не менее, мы должны критически проанализировать как его восприятие, так и его сильные и слабые стороны.

Посол Филипп Вервир сделал следующее заявление, выступая в Центре стратегических и международных исследований (CSIS) по теме «Геополитика управления Интернетом» 23 мая 2013 года:

«У нас в действительности нет определения процесса с участием всех заинтересованных сторон. *Я склонен думать о нем как о своего рода этосе инклюзивности, который с точки зрения понятия не предусматривает ничего другого, кроме указания направления* [выделено нами]. Мы должны попытаться добиться инклюзивности в той степени, в которой это возможно. Но существует множество особых ситуаций, в которых мы должны попытаться прийти к гораздо лучшему пониманию того, как мы собираемся обеспечить участие, и какие могут быть пределы широкого участия».

Как рассматривается ниже, основными недостатками управления Интернетом с участием всех заинтересованных сторон являются:

1. Отсутствие правил работы с участием всех заинтересованных сторон;
2. Воспринимаемое отсутствие подотчетности;
3. Слабая легитимность с точки зрения многих государств;
4. Неравномерность участия заинтересованных сторон, не являющихся поставщиками технологий.

Для управления Интернетом не существует формальных правил проведения встреч с участием всех заинтересованных сторон. Несмотря на то, что Инженерная рабочая группа Интернета представила нормы хорошего поведения, их механизмы принуждения сводятся к ограничению списков рассылки рабочей группы или давлению со стороны общественности — наказаниям, которые редко применяются. Это было приемлемо, поскольку работа Инженерной рабочей группы Интернета является добровольной, как и её «стандарты». Если человек не может добиться рассмотрения идеи в группе, он может пойти на другие форумы или создать свой, где его мнение может быть услышано, а «стандарт», возможно, принят.

Хотя ICANN характеризует себя как организацию с участием всех заинтересованных сторон, её устав не содержит правил проведения совещаний с участием всех заинтересованных сторон. Нет и положений для вынесения предложений на рассмотрение или для оспаривания кандидатур, которые предлагаются, например, Комитетом по назначениям. Аналогичным образом, хотя Комитет по назначениям выбирает 8 из 16 членов совета ICANN и членов других организаций ICANN, он не публикует свои методики отбора. Таким образом, регламент не отвечает на главный вопрос — как выбираются люди для работы в ICANN. Это способствует воспринимаемому отсутствию легитимности ICANN.

Для реализации функций Администрации адресного пространства Интернета (IANA) был заключен контракт ICANN с Министерством торговли США. В то время как некоторые государства раскритиковали эту связь, некоторая критика может прекратиться, ввиду того, что США планируют отказаться от своего контроля над функционированием IANA. Государства также выразили несогласие с некоторыми утвержденными ICANN Общими доменами высшего уровня.

Джим Льюис в недавней публикации (Lewis, 2013) комментирует легитимность управления Интернетом в целом [выделено нами].

«*Существующий подход к управлению Интернетом является политически несостоятельным, потому что ему не хватает легитимности в глазах многих новых интернет-пользователей*».

«Источником легитимности в существующей модели управления являлись технические знания. Сейчас это замещается политическими процессами. В то время как *существующая неформальная модель с участием всех заинтересованных сторон должна быть преобразована...* по-прежнему неясно, что придёт на смену этим процессам... *есть реальный риск, что любое изменение может привести к тому, что Интернет станет менее свободным... инновационным и... полезным для народов мира*».

В этой статье мы говорим, что организация является легитимной, если является эффективной, подотчетной и соответствует общепринятым ценностям и ожиданиям. Под *эффективностью* мы понимаем успешное достижение желаемых результатов при минимизации нежелательных последствий. Эта характеристика предполагает наличие как гибкости, так и эффективности. Под *подотчетностью* мы понимаем, что организация обладает прозрачностью и последовательностью. (Андреас Шедлер говорит об этих признаках, как «подотчетности» и «обеспечении исполнения». [Schedler, 1999]) Прозрачность означает, что члены организации, участники, граждане или их представители могут наблюдать за тем, что делается от их имени. Последовательность означает, что есть предсказуемые и единообразные санкции против ненадлежащего поведения тех, кто осуществляет полномочия от имени учреждения. *Соответствие ценностям* означает воплощение всё более общепринятых ценностей и ожиданий, в том числе инклюзивности, участия и взаимности. Только в том случае, если институты управления будут демонстрировать эти характеристики, люди начнут им доверять и легитимизируют их. А в условиях «глобальной деревни» легитимность становит-

ся необходимой для успешного выполнения государством своих функций.

Все национальные правительства, будь они демократическими или авторитарными, хотят участвовать в управлении Интернетом. Некоторые государства обеспокоены проблемами информационной безопасности, то есть контентом, который угрожает стабильности государства. Для других важны права человека; они обеспокоены, что государственная слежка вышла из-под контроля и необходимо ввести ограничения для информационных агрегаторов и поисковых сервисов. Третьи утверждают, что свобода выражения мнений является основополагающим фактором полной реализации преимуществ Интернета. На этих основаниях ведётся дискуссия по вопросам управления Интернетом.

Каким вопросам, связанным с Интернетом, необходимо управление?

Было множество призывов (Серф (Капур, 2005 г.) и Кастро и Аткинсон (Castro&Atkinson, 2014) упростить управление Интернетом путем передачи ответственности по отдельным вопросам политики соответствующим организациям. По этой проблеме Лаура ДеНардис говорит: «такой вопрос, как ‘кто должен контролировать Интернет — Организация Объединенных Наций или какая-либо другая организация’, не имеет смысла. Правильный вопрос подразумевает определение того, какая форма управления является наиболее эффективной в каждом конкретном контексте» (DeNardis, 2014, P226). Джозеф Най отмечает, что существует большая совокупность киберрежимов для решения многих вопросов, которые составляют управление Интернетом (Джозеф Най, 2014).

Най (Joseph Nye, 2014), Кастро и Аткинсон (Castro&Atkinson, 2014), и ДеНардис (DeNardis&Raymond, 2013) предлагают категории, на которые расщепляется управление Интернетом. Мы решили разложить его на следующие пять вопросов:

1. Вопросы сети
2. Управление контентом
3. Права человека
4. Киберпреступность
5. Кибератаки

Вопросы сети относятся к тем аспектам, которые имеют центральное значение для правильной работы Интернета. Они включают в себя присвоение имен и маршрутизацию, управле-

ние трафиком, сетевую безопасность, технические стандарты и торговые марки.

Хотя ICANN в целом хорошо справлялся с функцией присвоения имен, звучали призывы к укреплению его легитимности. Ввиду того, что Национальное управление США по телекоммуникациям и информационным технологиям (NTIA) объявило, что готово отказаться от контроля файла корневой зоны, подотчетность ICANN перед сообществом находится в стадии обсуждения. В рамках этого обсуждения мы предлагаем, чтобы Независимая комиссия по проверке также стала независимой от её Правления, а также в ней было обеспечено представительство государств, но, при этом, необходимо ограничить её полномочия, например, функциями выделения и перераспределения Общих доменов верхнего уровня и надзора за развертыванием стандартов DNS и BGP, а также за ключами, используемыми в обеспечении безопасности DNS и BGP. Управление трафиком в основном является национальным вопросом. Технические стандарты обрабатываются удовлетворительным образом более 200 организациями по всему миру и не нуждаются в изменении. Их принятие определяют рыночные силы. Вопросы, связанные с торговыми марками, которые возникают при распределении доменных имен, можно продолжать решать ситуативно в текущем порядке или посредством Всемирной организации интеллектуальной собственности (ВОИС), если возникнет общая проблема.

Управление контентом включает в себя неприкосновенность частной жизни, фильтрацию передаваемых данных (для предотвращения детской порнографии, спама или конкурирующих услуг, таких как VoIP), безопасность хранящейся и передаваемой информации, и локализацию данных.

Защита главным образом является национальным делом. Она становится международной проблемой, когда государство требует от местного провайдера обеспечить доступ к частной информации на компьютерах в иностранном государстве. Такие вопросы могут быть решены через Генеральную Ассамблею ООН (ГА ООН) или Всемирную торговую организацию (ВТО).

Государства оставляют за собой право контроля нежелательного контента, например, спама или детской порнографии. Трансграничное управление контентом является деликатным вопросом, когда возникает конфликт между такими национальными ценностями, как свобода слова и государственная безопасность. Когда возникают разногласия, Совет по правам человека является хорошим местом для их первичного обсуждения.

Интернет-провайдеры могут играть полезную роль в снижении спама. На самом деле, в их интересах делать это. Обмен между провайдерами Интернета передовым опытом по таким вопросам может осуществляться с помощью таких организаций, как сообщество Интернет или Форум групп реагирования на происшествия и обеспечения безопасности (FIRST).

Обеспечение безопасности хранимых данных в значительной степени является частным делом. Этот вопрос становится государственным, когда рассматриваемые данные касаются большей части граждан. Некоторые страны настаивают на локализации данных. Обеспечение безопасности передаваемой информации является как национальным, так и международным вопросом. Этот вопрос является внутренним, когда информация передаётся только внутри сетей на территории одного государства. Он становится международным, когда информация пересекает границы и когда она зашифрована. ВТО может быть лучшим местом для решения таких вопросов.

Государства заинтересованы в защите международных коммуникационных ресурсов, от которых они зависят, таких, как системы подводных кабелей. МСЭ является хорошим местом для обсуждения этого вопроса.

Права человека включают свободу выражения мнений и убеждений, экономические, социальные и культурные права, право на самоопределение и развитие, неприкосновенность частной жизни и наблюдение.

Вопросы, связанные с правами человека, могут в общем виде решаться внутри стран или через Совет по правам человека. Некоторые вопросы, такие как наблюдение, являются внутренними и международными. На международном уровне местом решения этих вопросов может быть ГА ООН.

Киберпреступность включает в себя преступления на почве ненависти, кибернасилие, детскую порнографию, мошенничество, хищение денежных средств и интеллектуальной собственности, хищение личных данных, получение несанкционированного доступа, повреждение оборудования и программного обеспечения, повреждение данных, повреждение физических систем, контролируемых с помощью Интернета, нарушение сетевого трафика и другие подобные деяния.

Учитывая глобальный охват Интернета, каждый из этих вопросов является внутренним и международным. Хотя Конвенция Совета Европы о киберпреступности действует в более чем 40 странах, такие важные государства, как Китай или Россия,

не приняли её. Тем не менее, эти страны осуществляют обмен некоторой информацией по киберпреступлениям. Региональные и международные организации, неправительственные организации, ШОС и комитеты ГА ООН являются площадками для дальнейшего расширения сотрудничества в этой области.

Кибератаки являются деятельностью, осуществляемой посредством телекоммуникационных сетей и которая причиняет серьезный ущерб государствам, национальным интересам или критически важным национальным инфраструктурам. Последние являются ресурсами, доступными через Интернет, необходимыми для функционирования современного общества, такими как газ, электричество, вода, пища, государственные и финансовые услуги, производство и медицинские учреждения. Учитывая, что посредством кибератак национальной экономике может быть нанесен серьёзный ущерб, страны должны принять меры, чтобы уменьшить риск возникновения подобной ситуации.

Первый комитет ГА ООН является подходящим местом для противодействия этим угрозам. Другие места включают в себя площадки, отмеченные Джозефом Наем (Joseph Nye, 2014), такие как G7, G20 и ОЭСР, группы государств и региональные организации подобные Совету Европы и Шанхайской организации сотрудничества.

Существуют другие вопросы управления Интернетом, которые не решаются никаким международным органом, например, безопасность цепи поставок. Для них государства должны попытаться либо расширить мандат таких существующих организаций, как Всемирная торговая организация, или заключить договора о взаимной юридической помощи.

Некоторые вопросы управления Интернетом носят в первую очередь технический характер. Такие вопросы должны принимать во внимание мнение технических экспертов. Политики не должны изменять технические рекомендации. Например, Софаэр и др. (Sofaer et al., 2010) предлагают ИКАО в качестве модели для управления Интернетом. ИКАО регулирует гражданскую, но не военную авиацию. Самое главное, что в ИКАО контроль над стандартами остаётся у профессионалов, а не политиков. Другими моделями могут быть Международная организация труда (МОТ), которая в настоящее время рассматривается Институтом Восток-Запад, и организации Красного Креста / Красного Полумесяца, которые в настоящее время рассматриваются комиссией Бильдта.

Управление с участием всех заинтересованных сторон было наиболее эффективным при развитии Интернета. Соответственно, по мере того как вопросы управления Интернетом переносятся в новые или существующие международные организации, в них должна быть интегрирована консультативная функция с участием всех заинтересованных сторон. Должны быть предоставлены новые возможности участия для Интернет-сообщества в широком смысле — в том числе правительств, гражданского общества, бизнеса, научных кругов и влиятельных Интернет-пользователей.

Выводы и предложения

Вопрос управления Интернетом нуждается в упрощении и уточнении. Следуя примеру других, мы рекомендуем упростить его путем разделения на темы, которые могут быть переданы существующим международным органам, таким, как СПЧ, ВОИС, ВТО, МСЭ, СЕ, а также государственным объединениям и региональным органам. Если этим организациям не хватает экспертных знаний об Интернете, это можно исправить. Технические вопросы в основном могут быть решены техническими организациями.

Когда существующие организации занимаются вопросами управления Интернетом, мы рекомендуем им использовать консультативные единицы с участием всех заинтересованных сторон, чтобы понять их мнение. Для многих технических и связанных с ними вопросов, в которых есть политическое измерение, мы рекомендуем добавление небольшого, тщательно организованного надзорного слоя с ограниченными полномочиями для проверки технических или смежных решений. Этот дополнительный слой будет обладать прозрачностью методов работы и независимостью членства. Он будет обладать правом одобрять или не одобрять, но не изменять технические или относящиеся к техническим решения технической организации. Небольшая организация с участием всех заинтересованных сторон может заняться созданием этого независимого надзорного слоя с участием представителей ключевых государств в киберпространстве, а также представителей корпораций, некоммерческих и технических организаций. Ключевой вопрос заключается в том, будут ли государства составлять большинство или множество (Бразильский Руководящий комитет Интернета (www.CGI.br) является моделью для такого органа).

Библиография

1. Akplogan, A., Curran, J., Wilson, P., Housley, R., Chehade, F., Arkko, J., Jaffe, J. (2013). The Montevideo Statement on the Future of Internet Cooperation.

2. Castro, D., & Atkinson, R. (2014). Beyond Internet Universalism: A Framework for Addressing Cross-Border Internet Policy, The Information Technology & Innovation Foundation. Retrieved from The Information Technology & Innovation Foundation website: http://www2.itif.org/2014-crossborder-internet-policy.pdf

3. Corwin, P. (2014). NETmundial Multistakeholder Statement Concludes Act One of 2014 Internet Governance Trifecta, Circle ID. (May 3, 2014). Retrieved from the Circle ID website: http://www.circleid.com/posts/20140504_netmundial_multistakeholder_statement_concludes_act_one_of_2014/

4. DeNardis, L., & Raymond, M. (2013). Thinking Clearly about Multistakeholder Internet Governance. Retrieved from the Social Science Research Network, SSRN 2354377: http://ssrn.com/abstract=2354377

5. DeNardis, L. (2014). The Global War for Internet Governance. New Haven: Yale University Press.

6. Hemmati, M. (2002). Multi-stakeholder Processes for Governance and Sustainability: Earthscan Publishing.

7. Huijstee, M. v. (2012). Multi-Stakeholder Initiatives: A Strategic Guide for Civil Society Organizations, The Social Science Research Network, SSRN 2117933. Retrieved from the website:Social Science Research Network, SSRN 2117933. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2117933

8. ICANNWiki. (2014). Multistakeholder Model. Retrieved from the ICANN website: http://icannwiki.com/index.php/Multistakeholder_Model

9. IETF. (2014). The IETF Process: an Informal Guide, IETF. Retrieved from their website: http://www.ietf.org/about/process-docs.html

10. Joseph Nye, J. (2014). The Regime Complex for Managing Cyber Activities, The Global Commission on Internet Governance. Retrieved from the Global Commission on Internet Governance their website: https://www.ourinternet.org/

11. Kapur, A. (2005). Internet Governance: A Primer: Reed Elsevier, India.

12. Kummer, M. (2013). Multistakeholder Cooperation: Reflections on the emergence of a new phraseology in international cooperation, Internet Society. Retrieved from their website: http://www.internetsociety.org/blog/2013/05/multistakeholder-cooperation-reflections-emergence-new-phraseology-international

13. Lewis, J. A. (2013). Internet Governance: Inevitable Transitions (Vol. 4): The Centre for International Governance Innovation. Retrieved from their website: https://www.cigionline.org/publications/2013/10/internet-governance-inevitable-transitions

14. Schedler, A. “Conceptualizing Accountability” The Self-Restraining State: Power and Accountability in New Democracies. Ed. Andreas Schedler, Larry Diamond, and Marc F. Plattner. Boulder and London: Lynne Rienner Publishers, 1999. 13–28.

15. Sofaer, A. D., Clark, D., & Diffie, W. (2010). Cyber Security and International Agreements. Proceedings of a Workshop o Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, 179 — 206, National Academies Press. Retrieved from their website: http://www.nap.edu/openbook.php?record_id=12997&page=179

16. Strickling, L. (2013). Moving Together Beyond Dubai, blogpost, The National Telecommunications and Information Adminstriation. Retrieved from http://www.ntia.doc.gov/blog/2013/moving-together-beyond-dubai

17. Vallejo, N., & Hauselmann, P. (2004). Governance and Multi-Stakeholder Processes, The International Institute for Sustainable Development s. Retrieved from the International Institute for Sustainable Development website: http://www.iisd.org/pdf/2004/sci_governance.pdf

18. WSIS. (2005). Tunis Agenda for the Information Society, International Telecommunications Union. Retrieved from the International Telecommunications Union website: http://www.itu.int/wsis/docs2/tunis/off/6rev1.html

John E.Savage
Brown University

Bruce W.McConnell
EastWest Institute

Exploring Multi-Stakeholder Internet Governance[1]

Abstract

Interest in Internet governance has been fueled by media attention to cyber crime, global surveillance, commercial espionage, cyber attacks, and threats to critical national infrastructures. Many nations have decided that they need more control over Internet-based technologies and the policies that support them. Others, emphasizing the positive aspects of these technologies, argue that traditional systems of Internet governance, which they label "multi-stakeholder" and which they associate with the success of the Internet, must continue to prevail.

In this paper we provide background on multi-stakeholder governance as it has been practiced in other fields for decades. We then examine multi-stakeholder Internet governance.

Three recommendations are made. First we propose simplifying Internet governance (IG) by partitioning it into issues that can be addressed by existing international agencies and those that cannot. The latter include naming, routing, security, and standards. These are primarily technical issues but have a policy dimension. Second, for bodies handling technical or technically related issues, such as the Internet Corporation for Assigned Names and Numbers (ICANN), we recommend adding a multi-stakeholder oversight layer that can accept or reject opinions from these bodies but not alter them. Third, existing international agencies handling other issues should be altered to receive Internet community input through multi-stakeholder consultative processes. With these changes IG can be made more comprehensive and manageable while protecting its most valuable characteristics.

Introduction

Interest in Internet governance (IG) has grown steadily since the creation of the Internet Corporation for Assigned Names and Numbers

[1] This is an abbreviated version of a longer paper published by the EastWest Institute.

(ICANN) in 1998 and is now discussed at many international forums. The World Summit on the Information Society (WSIS), held in 2003 and 2005, was a landmark event. Paragraph 34 of the 2005 Tunis Agenda (WSIS, 2005), contains the following working definition of IG.

A working definition of Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.

The Secretary General of the UN created the Internet Governance Forum (IGF) as an offshoot of WSIS and has met annually since 2006. It provides an important venue for thousands of participants to share ideas on Internet governance but has no authority to make recommendations.

In 2013 the leading Internet organizations met in Montevideo (Akplogan et al., 2013) and "identified the need for (an) ongoing effort to address Internet Governance challenges, and agreed to catalyze community-wide efforts towards the evolution of global multi-stakeholder Internet cooperation."

This meeting led to the April 2014 NETmundial: The Global Multi-stakeholder Meeting on the Future of Internet Governance (ICANNWiki, 2014) held in Brazil. It produced a set of principles and a roadmap for the evolution of the Internet that were endorsed by most participants, but not China, India, or Russia. They prefer a "UN-led, government centric approach to Internet governance" (Corwin, 2014).

One NETmundial Internet governance process principle states "Internet governance should be built on democratic multi-stakeholder processes, ensuring the meaningful and accountable participation of all stakeholders, including governments, the private sector, civil society, the technical community, the academic community and users."

The multi-stakeholder model is now widely touted as the IG model of choice. The White House endorsed it in its 2011 International Strategy for Cyberspace, as did both houses of the U.S. Congress in late 2012. ICANN describes itself as multi-stakeholder (ICANNWiki, 2014) while the International Telecommunications Union (ITU) says in a document published for the 2013 World Telecommunications Policy Forum (WTPF), "Through its Plenipotentiary Resolutions, the ITU membership recognizes the multi-stakeholder governance model based on the WSIS principles as the framework for global Internet governance" ("Supporting Multi-stakeholderism in Internet Governance," 2013).

Given the prominence that multi-stakeholder Internet governance has assumed, it is important to understand what the concept means, explore its strengths and weaknesses, and understand how best to implement it. It is imprudent for the world community to adopt this form of governance of a global resource as important as the Internet without first having a solid understanding of these issues.

Multi-stakeholder initiatives (MSIs) are attractive because they can provide an alternative between the extremes of laissez-faire policies and government regulation by enabling cooperation between NGOs and corporations in a form of self-regulation.

Unfortunately, there is no universally accepted definition of multi-stakeholder governance. The concept came into use as a vehicle for cooperation in the solution of societal problems, such as sustainability of natural resources and protection of workers in the developing world.

We now provide a brief history of IG; report on generic studies of multi-stakeholder initiatives; and examine the current problematic state of IG. We also give a detailed breakdown of IG issues and illustrate our proposed simplification of IG by allocating issues to existing international bodies. For technical issues, we recommend that if a political layer is attached to an existing body, such as ICANN, that it protect technical judgments from modification by the political layer. For non-technical IG issues, we recommend addition of multi-stakeholder components to international bodies that take responsibility for an IG issue.

Brief History of Internet Governance

The origins of the Internet as a DARPA research project are well known. The popularity of ARPANET and its successor, the Internet, led to its global proliferation. The Internet Engineering Task Force (IETF) emerged as a vehicle for researchers to discuss and seek endorsement of new network technologies without involving DARPA program managers. The World-Wide Web Consortium (W3C) emerged to serve a similar role for web-based technologies. It should be noted that to be a credible participant in these bodies requires in-depth knowledge of the technologies in question.

The IETF has created an informal but well-articulated system to guide its work. Its recommendations are recorded in thousands of documents called Request for Comments (RFCs). RFC 7154 explains the IETF code of conduct, namely, that participants are expected to show respect and courtesy to one another, have impersonal discussions,

come prepared to contribute, and work together to devise solutions for the global Internet. RFCs become de facto standards if widely adopted by multiple vendors.

The open, inclusive, transparent and permission-less philosophy that has characterized the creation of Internet technologies has encouraged the participation of engineers in their development and that of users in the creation of web content.

The Internet governance domain is very complex and has many players. What is remarkable is that it is reliably serving a population estimated at more than three billion users. In light of this, attempts to replace important parts of the current governance system must be done with great care. Another conclusion is that the Internet domain is likely too complex to be managed by one organization. It functions well because of the expertise that is distributed among the many players.

What is Multi-Stakeholder Internet Governance?

The term multi-stakeholder governance (MSG) was used for the Internet around 2004. Markus Kummer describes it as a vehicle "for policy dialogue where all stakeholders took part on an equal footing" via a process that is open, inclusive and transparent (Kummer, 2013). "While multistakeholder participation in the Working Group on Internet Governance (WGIG) and IGF meant and means that all stakeholders participate on an equal footing, it is also clear that in most organizations, whether intergovernmental or not, some structures are in place to facilitate decision-making processes" (Kummer, 2013).

Lawrence E Strickling, Administrator of the National Telecommunications & Information Administration (NTIA) in the U.S. Department of Commerce, says "the multistakeholder process ... involves the full involvement of all stakeholders, consensus-based decision-making and operating in an open, transparent and accountable manner."

These descriptions do not specify principles for the creation of multi-stakeholder organizations except to say that they should be open, transparent and inclusive. They don't specify how business is to be conducted except to say that "stakeholders participate on an equal footing" or that decisions are to be "consensus-based." These omissions call into question whether these descriptions of multi-stakeholder processes provide a sufficient basis on which to construct a global Internet governance system. We now examine multi-stakeholder initiatives in areas other than Internet governance.

Studies of Generic Multi-Stakeholder Governance

Minu Hemmati (Hemmati, 2002) explains that multi-stakeholder processes (MSPs) have been used for decades to address problems in a variety of areas including biotechnology, corporate conduct, energy, gender inequality, tourism, labor, mining, paper, and sustainability. She notes that MSPs inform decision makers on issues, generate support for decisions, identify solutions to problems, and encourage stakeholders to take ownership of issues. It has been effective in many social, political, economic and technical contexts, especially when the problems that arise are new, fast changing, and complex with important social and cultural dimensions. In these contexts, governments are typically slow to act. Through stakeholder engagement, MSG can quickly access the talent needed to address challenging new problems.

After studying 20 different multi-stakeholder processes, Hemmati (Hemmati, 2002) defines MSPs as "processes which aim to bring together all major stakeholders in a new form of communication, decision-finding (and possibly decision-making) on a particular issue. They are also based on recognition of the importance of achieving equity and accountability in communications between stakeholders and their views. They are based on democratic principles of transparency and participation and aim to develop partnerships and strengthened networks among stakeholders." She also says "MSPs cover a wide spectrum of structures and levels of engagement. They can comprise dialogues on policy or grow to include consensus-building, decision-making, and implementation of practical solutions. ... Hence, MSPs come in many shapes."

She cautions that "MSPs are not a universal tool or panacea for all kinds of issues, problems and situations. They are akin to a new species in the system of decision-finding and governance structures and processes. They are suitable for those situations where dialogue is possible and where listening, reconciling interests and integrating views into joint solution strategies seems appropriate and within reach." Citing Kader Asmal concerning a debate over dams, she warns us, "More often, [than not] the process becomes a messy, loose-knit, exasperating, sprawling cacophony. Like pluralist democracy, it is the absolute worst form of consensus-building except for all the others."

Hemmati (Hemmati, 2002) observes that creating an MSP requires decisions concerning the secretariat, the physical support for the organization, funding, reporting and documentation, contact with the public, and whether and how there will be linkage into an official

decision-making process. More specifically she notes that a wide range of decisions are needed including: a) identifying the issues to be addressed; b) deciding which stakeholders to invite; c) whether attendance is by invitation only, open to all or to a limited representation from each stakeholder group; d) setting timetables for action; e) preparing for meetings; f) communications between stakeholders, e.g. via the web or local, regional, or broader meetings; g) addressing power gaps between stakeholders as a result of expertise or access to funds; h) whether and/or how to make recommendations and/or decisions (is consensus required?); and, i) the conditions under which to terminate an MSP.

Vallejo et al. (Vallejo & Hauselmann, 2004) observe that many NGOs and business initiatives have emerged that deal with voluntary, non-state "standard setting, certification and labeling activities, collaborative arrangements for sector specific policy-making, supply chain management interventions, or ... codes of conduct". While their analysis of multi-stakeholder initiatives is less comprehensive than Hemmati's, they observe that viability of such initiatives is strongly dependent on their legitimacy and efficiency. They cite Suchmann's 1995 definition of legitimacy as "a generalized perception or assumption that the actions of an entity are desirable, proper and appropriate within some socially constructed system of norms, values, beliefs and definitions."

In a thoughtful and insightful 2012 study van Huijstee (Huijstee, 2012) offers a strategic guide for civil society organizations (CSOs) who intend to participate in multi-stakeholder initiatives (MSIs) designed to encourage corporations to manage natural resources in a more sustainable manner. She provides advice concerning many aspects of organizing MSIs. She says that the possible role of governments needs to be understood noting "MSIs are, by their very nature, instruments of civil (or self-regulation from the perspective of business)." "Government agencies may play an endorsing, convening, facilitating or financing role in MSIs, but often they will not be comfortable negotiating standards with CSOs or businesses." She also says, "In the longer term, MSIs may serve as experimental mechanisms that start as voluntary initiatives but slowly get transcribed into governmental policies and regulation along the way." We turn now to an analysis of Internet governance.

The Scope of Internet Governance

Most proposals for multi-stakeholder Internet governance include too many topics. This is illustrated by the 2014 IGF Istanbul meeting. Discussions were held on access to the Internet, freedom of expres-

sion, child safety, privacy, the economics of the open Internet, IPv6 deployment, accessibility to IGF by persons with disabilities, the "right to be forgotten", gender issues, climate change, the Internet of things, human rights, public access to libraries, the mobile Internet, and a safe, secure and sustainable Internet. If Internet governance is to be manageable, the problem must be simplified.

In his preface to (Kapur, 2005),Vint Cerf addresses this issue by saying "With few exceptions, most of the public policy issues associated with the Internet lie outside the purview of ICANN and can and should be addressed in different venues. For example, spam, and its instant messaging and Internet telephony relatives ... may only be successfully addressed through legal means, although there are some technical measures that can be undertaken by Internet Service Providers (ISPs) and end users to filter out the unwanted messages. Similarly fraudulent practices such as 'phishing' and 'pharming' may best be addressed through legal means. Intellectual property protection may, in part, be addressed through the World Intellectual Property Organization (WIPO) and business disputes through the World Trade Organization (WTO) or through alternative dispute resolution methods such as mediation and arbitration." We explore the disaggregation of Internet governance into separate topics below. Before doing that, we examine problems that others have with the state of Internet governance.

The Current State of Internet Governance

Multi-stakeholder governance engages stakeholders who bring their expertise and enthusiasm to bear either on the generation of new technologies or web content. Not only is this process more responsive than governments, it has been a driver of innovation and economic stimulation. Nonetheless, we need to critically examine both the way it is perceived as well as its strengths and weaknesses.

Ambassador Philip Verveer made the following statement at a panel at the Center for Strategic and International Studies (CSIS) on The Geopolitics of Internet Governance on May 23, 2013:

«We really don't have a definition of the multi-stakeholder process. I tend to think of it as a kind of ethos of inclusivity, which doesn't provide much other than guidance in terms of the notion. [Emphasis added.] To the extent that inclusivity is possible, we ought to try to achieve it. But there are a lot of specific contexts where we have to try to come to a much better understanding about how we're going to enable participation and what the limits of broad participation may be".

As discussed below, the principal weaknesses in multi-stakeholder Internet governance are the following:

1. Absence of rules for multi-stakeholder operation,
2. A perceived lack of accountability,
3. Weak legitimacy in the eyes of many states, and
4. Uneven engagement of stakeholders who are not technology providers.

Formal rules for running multi-stakeholder meetings don't exist for Internet governance. Although the IETF has stated norms for good behavior, their enforcement mechanisms are limited to reducing participation in working group mailing lists or peer pressure, punishments that are rarely invoked. This has been acceptable because the work of IETF is voluntary as are its "standards." If an individual cannot get a hearing for an idea at IETF, they can move to or create other forums where their views can be heard and a "standard" possibly adopted.

Although ICANN characterizes itself as multi-stakeholder, its bylaws do not provide rules for the conduct of multi-stakeholder meetings. No provisions exist to make motions or challenge nominations that emerge from the Nominating Committee, for example. Similarly, although the Nominating Committee selects 8 of the 16 members of the ICANN board and members for other ICANN organizations, it does not publish its selection procedures. Thus, on the central question of how individuals are chosen to run ICANN, the bylaws are silent. This contributes to ICANN's perceived lack of legitimacy.

ICANN is under contract with the U.S. Department of Commerce for administration of the Internet Assigned Numbers Authority (IANA) functions. While some governments have criticized these ties, since U.S. is planning to relinquish its oversight of IANA functions, some of these criticisms may disappear. Governments have expressed opposition some ICANN-approved Generic Top Level Domains (gTLDs).

Jim Lewis comments on the legitimacy of Internet governance in general in a recent paper (Lewis, 2013). (Emphasis added.)

"The current approach to Internet governance is politically untenable because it lacks legitimacy in the eyes of many new Internet users."

"The source of legitimacy in the existing governance model was technical expertise. This is now being displaced by political processes. While the current, informal multi-stakeholder model must be transformed ... What will replace these processes remain(s) unclear ... there is real risk that any transition could lead to an Internet that is less free, ... innovative and ... valuable to the nations of the world."

In this paper we say that an organization is legitimate if it is effective, accountable, and aligned with its constituents' values and expectations. By effective, we mean good at delivering desired results, while minimizing undesired consequences. This characteristic assumes both agility and efficiency. By accountable, we mean the institution exhibits transparency and consequence. (Andreas Schedler refers to these traits as "answerability" and "enforcement." [Schedler, 1999]) Transparency means that its constituents, members, citizens, or their representatives, can see what is being done in their name. Consequence means there are predictable and consistent sanctions against bad behavior by those who exercise power in the name of the institution. Alignment with constituent values means embodying values and expectations that are increasingly commonly held, including inclusiveness, participation, and reciprocity. Only when governance institutions demonstrate these characteristics will people put their trust in them, legitimize them. And, in the global village, legitimacy is becoming essential to government's successful fulfillment of its purpose.

Whether democratic or autocratic, national governments want a voice in Internet governance. Some nations are concerned about information security, that is, content that threatens state stability. Others are concerned about human rights; worrying that surveillance by states has gotten out of hand and those restrictions are needed on information aggregators and search providers. Still others insist that freedom of expression is fundamental to realizing the full benefit of the Internet. For these reasons, the debate on Internet governance is engaged.

What Internet Issues Need Governing?

Calls have been made by Cerf (Kapur, 2005) and Castro and Atkinson (Castro & Atkinson, 2014) to simplify Internet governance by allocating responsibility for individual policy issues to relevant organizations. On this issue Laura DeNardis says "a question such as 'who should control the Internet, the United Nations or some other organization' makes no sense whatsoever. The appropriate question involves determining what is the most effective form of governance in each specific context" (DeNardis, 2014, p226). Joe Nye observes that a large cyber regime complex exists to address many issues that constitute Internet governance (Joseph Nye, 2014).

Nye (Joseph Nye, 2014), Castro and Atkinson (Castro & Atkinson, 2014), and DeNardis (DeNardis & Raymond, 2013) propose categories into which to decompose Internet governance. We have chosen to decompose it into the following five topics:

1. Network Issues
2. Content Control
3. Human Rights
4. Cyber Crime
5. Cyber Attacks

Network issues refers to those matters central to the proper operation of the Internet. They include naming and routing, traffic management, network security, technical standards and trademarks.

Although ICANN has generally handled naming functions well, there have been calls to strengthen its legitimacy. Because NTIA has announced that it is willing to give up its supervision of the root zone file, the accountability of ICANN to its community is under discussion. We add to that discussion by suggesting that its Independent Review Panel (IRP) be made independent of its board and provide for representation of states but that its oversight be circumscribed to include, for example, the allocation and de-allocation of gTLDs and the supervision of the deployment of DNS and BGP standards as well as the keys used in securing DNS and BGP. Traffic management is largely a domestic issue. Technical standards are handled in a satisfactory manner by more than 200 organizations worldwide and don't need to be changed. Market forces determine adoption. Trademarks issues that arise in domain name allocation can continue to be addressed in the current ad hoc manner or be referred to the World Intellectual Property Organization (WIPO) if a generic issue is identified.

Content control includes privacy, filtering of data in transit (to prevent child pornography, spam or competing services, such as VOIP), security of data at rest and in motion, and data localization.

Privacy is primarily a domestic issue. It becomes international when a nation commands a domestic ISP to make available private information on computers in a foreign state. Such matters can be handled in the UN General Assembly (UNGA) or the World Trade Organization (WTO).

Nations reserve the right to control of undesirable content, such as spam or child pornography. Trans-border control of content is a delicate matter when national values are in conflict, such as freedom of speech versus state security. When disagreements arise, the Human Rights Council is a good first place to air them.

ISPs can play a useful role in reducing spam. In fact, it is often in their interest to do so. Sharing of ISP best practices on such issues can be done via organizations such as the Internet Society or FIRST, the incident response organization.

Securing data at rest is largely a private matter. It is national when the data in question concerns a large fraction of its citizenry. Some nations insist on data localization. Securing data in motion is both a domestic and an international issue. It is domestic when the data transits only domestic networks. It becomes international when it crosses boundaries and when it is encrypted. The WTO may be the best venue for such matters.

Nations have an interest in protecting international communication resources on which they rely, such as the undersea cable systems. The ITU is an good venue for this issue.

Human rights include freedom of expression and belief, economic, social and cultural rights, the right to self-determination and development, privacy, and surveillance.

Human rights issues can generally be decided either domestically or via the Human Rights Council (HRC). Some issues, such as surveillance, are both domestic and international. At the international level, UNGA may be the venue to address the latter.

Cyber crime includes hate crimes, cyber bullying, child pornography, fraud, theft of cash and intellectual property, identity theft, unauthorized trespass, damage to hardware and software, data corruption, damage to physical systems controlled via the Internet, disruption of network traffic, and other similar activities.

Given the global reach of the Internet, each of these issues is both domestic and international. Although the Council of Europe Convention on Cybercrime is in effect in more than 40 countries, important countries such China or Russia have not adopted it. Nonetheless, these countries do share some cyber crime information. Regional and international organizations, NGOs, SCO, and UNGA committees are venues to further expand cooperation in this area.

Cyber attacks are actions via networks that cause serious damage to a nation, national interests, or critical national infrastructures. The latter are resources accessible via the Internet essential to the functioning of modern societies, such as gas, electricity, water, food, government and financial services, manufacturing, and medical facilities. Given that a national economy can be severely damaged by a cyber attack, nations must take steps to reduce the risk of this occurring.

The UNGA First Committee is an appropriate venue to address these threats. Other venues include the regimes identified by Joe Nye (Joseph Nye, 2014), such as the G7, G20, and OECD, government groupings, and regional organizations, such as the Council of Europe and the Shanghai Cooperation organization.

Other Internet governance issues exist that are not addressed by any international body, such as security of the supply chain. For these, nations should try to either extend the mandate of existing organizations, such as the World Trade Organization, or create mutual legal assistance treaties (MLATs) for this purpose.

Some governance matters are primarily technical in nature. Such matters must respect the judgments of technical experts. Politicians should not modify technical recommendations. For example, Sofaer et al (Sofaer et al., 2010) propose ICAO as model for Internet governance. ICAO regulates civil but not military aviation. Most importantly, in ICAO professionals retain control over standards, not the policy makers. Other models may be the International Labor Organization (ILO), which is being examined by the EastWest Institute, and the Red Crescent/Red Cross, which is being examined by the Bildt Commission.

Multi-stakeholder governance has been most effective in the development of the Internet. Thus, as Internet governance issues are allocated to new or existing international organizations, a multi-stakeholder consultative function should be grafted onto them. New opportunities must be provided for the Internet community, broadly interpreted, to participate. This includes governments, civil society, business, academia, and important Internet users.

Conclusions and Recommendations

Internet governance is a topic in need of simplification and refinement. Following the lead of others, we recommend that it be simplified by disaggregating it into topics that can be handled by existing international bodies, such as the HRC, WIPO, WTO, ITU, CoE as well as government groupings and regional bodies. If these organizations lack expert knowledge of the Internet, this can be remedied. Technical issues can largely be handled by technical organizations.

When existing organizations are handling Internet governance matters, we recommend they invoke multi-stakeholder consultative units to seek the opinions of Internet stakeholders. For the many technical and technically related issues with a policy dimension, we recommend the addition of a small carefully crafted oversight layer with limited authority to validate the technical or technically related decisions. This additional layer would exhibit the qualities of transparency in its operating methods and independence in its membership. It would have the power to approve or disapprove, but not to modify, the technical or technically related decisions of the technical organization. A small,

multi-stakeholder body could undertake the creation of this independent review layer with representation from key state cyber powers supplemented by corporate, nonprofit, and technical representatives. A key question will be whether states constitute a majority or a plurality. (The Brazilian Internet Steering Committee (www.CGI.br) provides a model for this kind of body.)

Bibliography

1. Akplogan, A., Curran, J., Wilson, P., Housley, R., Chehade, F., Arkko, J., Jaffe, J. (2013). The Montevideo Statement on the Future of Internet Cooperation.
2. Castro, D., & Atkinson, R. (2014). Beyond Internet Universalism: A Framework for Addressing Cross-Border Internet Policy, The Information Technology & Innovation Foundation. Retrieved from The Information Technology & Innovation Foundation website: http://www2.itif.org/2014-crossborder-internet-policy.pdf
3. Corwin, P. (2014). NETmundial Multistakeholder Statement Concludes Act One of 2014 Internet Governance Trifecta, Circle ID. (May 3, 2014). Retrieved from the Circle ID website: http://www.circleid.com/posts/20140504_netmundial_multistakeholder_statement_concludes_act_one_of_2014/
4. DeNardis, L., & Raymond, M. (2013). Thinking Clearly about Multistakeholder Internet Governance. Retrieved from the Social Science Research Network, SSRN 2354377: http://ssrn.com/abstract=2354377
5. DeNardis, L. (2014). The Global War for Internet Governance. New Haven: Yale University Press.
6. Hemmati, M. (2002). Multi-stakeholder Processes for Governance and Sustainability: Earthscan Publishing.
7. Huijstee, M. v. (2012). Multi-Stakeholder Initiatives: A Strategic Guide for Civil Society Organizations, The Social Science Research Network, SSRN 2117933. Retrieved from the website:Social Science Research Network, SSRN 2117933. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2117933
8. ICANNWiki. (2014). Multistakeholder Model. Retrieved from the ICANN website: http://icannwiki.com/index.php/Multistakeholder_Model
9. IETF. (2014). The IETF Process: an Informal Guide, IETF. Retrieved from their website: http://www.ietf.org/about/process-docs.html
10. Joseph Nye, J. (2014). The Regime Complex for Managing Cyber Activities, The Global Commission on Internet Governance. Retrieved from the Global Commission on Internet Governance their website: https://www.ourinternet.org/
11. Kapur, A. (2005). Internet Governance: A Primer: Reed Elsevier, India.
12. Kummer, M. (2013). Multistakeholder Cooperation: Reflections on the emergence of a new phraseology in international cooperation, Internet Society.

Retrieved from their website: http://www.internetsociety.org/blog/2013/05/multistakeholder-cooperation-reflections-emergence-new-phraseology-international

13. Lewis, J. A. (2013). Internet Governance: Inevitable Transitions (Vol. 4): The Centre for International Governance Innovation. Retrieved from their website: https://www.cigionline.org/publications/2013/10/internet-governance-inevitable-transitions

14. Schedler, A. "Conceptualizing Accountability" The Self-Restraining State: Power and Accountability in New Democracies. Ed. Andreas Schedler, Larry Diamond, and Marc F. Plattner. Boulder and London: Lynne Rienner Publishers, 1999. 13–28.

15. Sofaer, A. D., Clark, D., & Diffie, W. (2010). Cyber Security and International Agreements. Proceedings of a Workshop o Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, 179 — 206, National Academies Press. Retrieved from their website: http://www.nap.edu/openbook.php?record_id=12997&page=179

16. Strickling, L. (2013). Moving Together Beyond Dubai, blogpost, The National Telecommunications and Information Adminstriation. Retrieved from http://www.ntia.doc.gov/blog/2013/moving-together-beyond-dubai

17. Vallejo, N., & Hauselmann, P. (2004). Governance and Multi-Stakeholder Processes, The International Institute for Sustainable Development s. Retrieved from the International Institute for Sustainable Development website: http://www.iisd.org/pdf/2004/sci_governance.pdf

18. WSIS. (2005). Tunis Agenda for the Information Society, International Telecommunications Union. Retrieved from the International Telecommunications Union website: http://www.itu.int/wsis/docs2/tunis/off/6rev1.html

Дэниел Штауффахер
Фонд ICT4Peace (Швейцария)

Роль гражданского общества в укреплении мер доверия

Мы, несомненно, живем в момент значительных изменений, в результате которых ряд обстоятельств привел к потере общественного доверия. Некоторая деятельность государств, в том числе негативное использование информационно-коммуникационных технологий (ИКТ) для достижения политических, военных и экономических целей, всё чаще бросает вызов связям между государствами, с одной стороны, и между государством и гражданами, с другой. Действительно, государства и негосударственные субъекты все чаще используют ИКТ для получения преимуществ в ходе вооруженных конфликтов или ситуациях напряженной политической конкуренции.

Существующее положение дел сформировалось в момент обширных и сложных изменений в системе международных отношений после Холодной войны — изменений, для которых оказалось трудно найти решения. Оно также появилось в то время, когда значительно снизилось доверие граждан к действиям государственных деятелей (и политиков). Свидетельства этого недоверия появились в различных регионах в конце первого десятилетия 2000-х годов и вылились в призывы к расширению демократического представительства и более эффективному управлению. Ситуация несколько обострилась после разоблачения практики бесконтрольного мониторинга и наблюдения, проводимого рядом государств, в том числе демократических.

Несмотря на это, на протяжении нескольких лет некоторые государства принимали участие в политических дискуссиях по вопросам норм, наращивания потенциала и развития мер доверия, направленных на снижение риска и укрепление доверия между государствами в связи с использованием информационных и коммуникационных технологий (ИКТ) в контексте международной и региональной безопасности. В 2013 году по итогам трудных переговоров был достигнут прорыв — Группа правительственных экспертов ООН (ГПЭ) и Организация по безопасности и сотрудничеству в Европе (ОБСЕ) выработали предварительное соглашение о содержании некоторых из этих норм, мер доверия и мер наращивания потенциала. Однако предметные дискуссии

о том, как они должны применяться и внедряться, находятся на ранней стадии. Более того, многие из продолжающихся попыток достижения консенсуса столкнулись с трудностями, прежде всего потому, что сложно (однако не невозможно) вписать ИКТ в традиционные парадигмы безопасности. Тем не менее, большинство государств признает ту роль, которую нормы и меры укрепления доверия могут сыграть в укреплении доверия между государствами и внутри государств. Кроме того, такие основные принципы управления как участие, транспарентность и подотчетность могут помочь построить и углубить доверие между государствами, а также между государствами и гражданами. Для этого правительства признали необходимость укрепления доверия и углубления их взаимодействия с другими группами — в том числе с общественными организациями — по мере дальнейшего формирования и внедрения новых норм и правил в этой области.

Участие гражданского общества в вопросах международного управления и безопасности не является чем-то новым, и существует множество примеров сфер деятельности, в которых государства создали такое взаимодействие. Более того, подобное участие помогло достигнуть положительных результатов, и, в частности, международное право и международное гуманитарное право извлекли значительную пользу из вклада общественных организаций. Они способствовали укреплению доверия между государствами и внутри государств (часто путем организации и участия в мероприятиях по укреплению мер доверия в форматах трек 1.5 и трек 2, и развивая диалог между сторонами), а также содействовали заключению договоров и созданию новых международных организаций, и лоббировали в государствах за поддержку более сильных международных норм и стандартов. Международная кибербезопасность не должна быть исключением. Более того, эта область по самой своей природе и ввиду широкого круга нормативных проблем требует гораздо более глубокого участия, чем в других областях.

Тем не менее, на сегодняшний день участие гражданского общества в формировании национальных стратегий кибербезопасности и региональных и международных норм и процессов построения мер укрепления доверия является минимальным, несмотря на то, что общественные организации, наряду с частным сектором, научным сообществом и аналитическими центрами являются основными звеньями в цепи создания ценности ИКТ, и у них есть «нормативные интересы» в отношении того, как будут решены международные и региональные проблемы безопас-

ности, связанные с ИКТ. Действительно, опыт, знания и охват этих групп имеет основополагающее значение для решения или реагирования на множество основных технических проблем, присущих ИКТ-среде, а также преодоления незащищенности и недоверия, сложившихся между странами и внутри них в отношении использования ИКТ.

В особенности гражданское общество может внести свой вклад, разрабатывая стратегии своего эффективного участия в текущих процессах, а именно, поддерживая и контролируя исполнение доклада ГПЭ 2013 года и внедрение первичных мер доверия ОБСЕ. В докладе ГПЭ, в частности, выделен ряд областей, в которых существующие нормы и процессы построения мер доверия могут получить значительную выгоду от более активного участия гражданского общества (а также частного сектора и научного сообщества). И хотя ОБСЕ не выделила роль гражданского общества (как не сделал этого в данном вопросе и АСЕАН) в формировании или реализации мер доверия, в работе этой организации существует достаточно прецедентов, демонстрирующих то, как важно участие гражданского общества и как оно может значительно повысить легитимность процессов, результат которых затрагивает все общество. В дополнение к непосредственному участию, общественные организации также могут выступать в поддержку большей прозрачности и подотчетности со стороны правительств, например, указывая области, где был достигнут успех, и призывая национальных лидеров к действию там, где это требуется. Подобным образом они могут работать со всеми заинтересованными сторонами для развития технической и нормативной базы знаний, необходимой для формирования обоснованных политических решений.

При эффективном и последовательном подходе такое сотрудничество может улучшить качественное измерение многосторонних норм и процессов построения мер доверия, связанных с международной безопасностью и использованием ИКТ государствами, придавая им большую легитимность и устойчивость. Такое сотрудничество также способно гарантировать, что будут учтены более широкие нормативные интересы, и что при поиске решений будет использоваться правильный технический опыт. В совокупности, это может помочь построить доверие между государствами, а также между государствами и обществом.

Daniel Stauffacher
ICT4Peace Foundation (Switzerland)

The Role of Civil Society in Furthering CBMs

We are undoubtedly living through a moment of significant change whereby a series of developments have led to the loss of public trust. The links between states on the one hand, and between state and citizens on the other, are being increasingly challenged by a range of state practices, including the negative uses of information communications technologies (ICTs) to advance political, military and economic objectives. Indeed, states and non-state actors are increasingly using ICTs to ratchet the advantage during armed conflict or situations of tense political contestation.

This situation has emerged at a moment of broad and complex shifts in the post-cold war international order, solutions for which are proving difficult to shape. It has also emerged at a time when citizen trust in the behaviour of state actors (and politicians) has decreased considerably. Evidence of this mistrust became manifest in the calls for more enhanced democratic representation and more effective government across regions as the first decade of the 2000s drew to a close, and has been somewhat aggravated by the recent revelations of the unchecked monitoring and surveillance practices of a number of governments, democratic or not.

Notwithstanding, for several years a number of states have been engaging in a series of policy discussions over norms, confidence and capacity building measures aimed at lowering risk and building trust among states with regard to the use of information and communications technologies (ICTs) in the context of international and regional security. In 2013, representing a major breakthrough in what had heretofore been difficult negotiations, a UN Group of Governmental Experts (GGE) and the Organization for Security and Cooperation in Europe (OSCE) reached initial agreement on the nature of some of these norms, confidence and capacity building measures. Substantive discussions on how these should be applied and implemented remain, however, at an early stage. Moreover, many of the on-going efforts to reach consensus have run into difficulty not least because it is hard (yet not entirely impossible) to fit ICTs into traditional security paradigms. Yet, most governments acknowledge the role norms and CBMs can play in strengthening trust between states and within states. In addi-

tion, core governance principles such as participation, transparency, and accountability can help build and deepen trust between states, and between states and citizens. To this end, governments have acknowledged the need to build trust and deepen their engagement with other groups — including civil society organisations — as they move to further shape and implement new norms and rules in this area.

Civil society engagement on international governance and security matters is not new, and there are scores of examples of areas in which states have accommodated such engagement. Moreover, this engagement has helped produce positive results, with international and international humanitarian law in particular benefitting enormously from the contribution of civil society organisations. The latter has helped build confidence between and within states (often through the organisation of and participation in track 1.5 and track 2 CBM processes and by fostering dialogue between parties), as well as fostering treaties, promoting the creation of new international organisations, and lobbying in national capitals to gain consent to stronger international rules and standards. International cyber security should not be an exception. Moreover, it is an area that, by its very nature and the broad range of normative concerns involved, calls for much deeper civil society engagement than experienced in other areas.

Yet, to date, civil society engagement in the shaping of national cyber security strategies or in regional and international norms and CBM processes has been minimal, despite the fact that civil society organisations represent, along with the private sector, academia and policy think-tanks, core links in the ICT value chain and have 'normative concerns' with regard to how ICT-driven international and regional security concerns are resolved. Indeed, the expertise, knowledge and reach of these groups is fundamental to resolving or responding to many of the core technical problems inherent in the ICT environment and many of the insecurities and mistrust that has emerged between and within states regarding the uses of ICTs.

In particular, civil society can contribute by developing strategies for their effective engagement in on-going processes, particularly with regard to supporting and monitoring implementation of the 2013 GGE Report and the OSCE's Initial Set of CBMs. The GGE Report in particular highlights a number of areas in which on-going norms and CBM processes would benefit significantly from greater involvement of civil society (as well as the private sector and academia). And while the OSCE has not identified a role for civil society (nor the ARF for that matter) in shaping or implementing CBMs, there is enough precedent in the work of that organisation to demonstrate how civil

society involvement is important and can add much more legitimacy to processes, the outcome of which affect all of society. In addition to direct engagement, civil society organisations can also advocate greater transparency and accountability on the part of governments, highlighting for example, where progress has been made and calling to task national leaders when required. They can similarly work with all relevant stakeholders to deepen the technical and normative knowledge base required to inform sound policy decisions.

If approached effectively and coherently, such engagement can improve the qualitative dimension of multilateral norms and CBM processes regarding international security and state uses of ICTs, affording them greater legitimacy and sustainability. It can also help ensure that broader normative concerns are attended to, and that the right technical expertise is leveraged when solutions are being sought. Combined, the latter can help build trust between states, and between states and society.

Р.А.Шаряпов

Институт проблем информационной безопасности
МГУ имени М.В.Ломоносова

Проблемы противодействия угрозам вмешательства во внутренние дела суверенных государств через социальные медиа

Уважаемые коллеги!

Сегодняшнее заседание посвящено весьма актуальной теме — проблеме противодействия угрозам вмешательства во внутренние дела суверенных государств через социальные медиа (экстремизм, радикализация и т.д.). Мы выносим на обсуждение следующие вопросы:

1. Социальные сети как новый феномен общественной жизни: плюсы и минусы.

2. Использование социальных медиа в деструктивных целях: анализ и прогноз тенденций.

3. Механизмы противодействия угрозам вмешательства во внутренние дела суверенных государств на национальном и международном уровне.

В настоящее время прослеживается устойчивая тенденция на повышение роли и значения социальных сетей, история которых началась в 1995 году с появлением американского портала Classmates.com. Любое общественно значимое событие сегодня обсуждается заинтересованными и активными пользователями в социальных сетях.

По прогнозам в 2015 г. число пользователей социальных сетей вырастет до 2,2 млрд (или 31% всего населения), расходы на рекламу в соц. сетях в 2014 г. составили более 15,3 млрд. долл.

Сегодня социальные сети, помимо выполнения функций поддержки общения по различным интересам, обмена мнениями, получения информации их членами, организации и ведения бизнеса, всё чаще становятся объектами и средствами информационно-психологического воздействия и управления на различных уровнях (в рамках региона, страны, международного сообщества). Сети, социальные медиа — это существенный инструмент деструктивного информационно-психологического влияния, в том числе — в целях манипулирования личностью, социальными группами и обществом в целом.

При этом отмечу, проблемы деструктивного использования Интернета и социальных сетей, как угрозы вмешательства во внутренние дела, актуальны, первую очередь, для государств с достаточным уровнем проникновения Интернета (по данным МСЭ к концу 2014 года Интернетом пользовались почти 3 миллиарда человек, или 42,3% населения планеты).

К сожалению, в настоящее время радикализация является динамичным расширяющимся процессом, проникающий во все социальные слои общества. И социальные сети используются в качестве главного инструмента распространения.

Отмечаемый всеми рост радикализации ведет к социализации экстремизма, что ложится в основу терроризма.

Недавние террористические акты в Европе потребовали пересмотра и активизации противодействия распространению этих идей, и в первую очередь, через соц. Сети.

В 2014 году «Исламское государство» (ИГ) использовало по меньшей мере 46 тысяч аккаунтов в Twitter, сообщает The Wall Street Journal со ссылкой на исследование Brookings Institution.

По последним исследованиям 2015 года Европарламента 90% всей террористической активности, включая пропаганду радикализма и экстремизма, ведется в Интернете с использованием социальных сетей.

Мировые лидеры, государственные деятели и руководители спецслужб имеют схожие позиции по проблеме распространения экстремистской идеологии через социальные сети.

Еще в ноябре 2014 г. директор Центра правительственной связи Великобритании (GCHQ) Роберт Ханниган (Robert Hannigan) писал, что ведущие социальные сети стали удобным плацдармом для террористических организаций, что террористы «Исламского государства» использовали возможности Интернета для создания глобальной международной террористической сети, а мессенджеры и социальные сети используются экстремистами для пропаганды своих идей и вербовки новых членов.

В феврале 2015 г. министр национальной безопасности США Джей Джонсон (Jeh Johnson) в интервью СМИ отметил, что по сравнению с планированием и организацией терактов 11 сентября, современные террористические организации более эффективно используют Интернет, социальные сети и другие средства для провокации индивидуальных терактов.

В ходе Саммита по противодействию насильственному экстремизму (февраль 2015 г., Вашингтон) и Президент США Барак Обама (Barack Hussein Obama), и Генеральный секретарь ООН

Пан Ги Мун (Ban Ki-moon), и Верховный представитель ЕС Федерики Могерини (Federica Mogherini) в своих выступлениях говорили о проблеме использования онлайн-СМИ и социальных сетей для распространяя идей экстремизма и терроризма, об идеологической обработке молодых людей и вербовке новых членов экстремистских и террористических групп, о распространении вируса страха.

По итогам Саммита (а в нем приняли представители органов государственной власти из более чем 60 стран мира, в том числе и директор ФСБ России А.В.Бортников) было озвучено совместное Заявление, в котором, как одно из направления деятельности, выделялось использование глобальных коммуникаций, в том числе и социальных медиа, чтобы противостоять агрессивным экстремистским сообщениям.

Напомню, что вчера на заседании нашего Форума Брюс Макконнелл (Bruce McConnell), рассказывая о приоритетах деятельности Института Восток-Запад, поставил проблему деструктивного контента на второе место.

В России также актуальна борьба с распространением идеологии радикализма и экстремизма в социальных сетях.

1 февраля 2014 года в России вступил в силу закон, позволяющий Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) по запросу Генеральной Прокуратуры без суда блокировать интернет-ресурсы с призывами к экстремизму и массовым беспорядкам. Ограничение доступа к таким сайтам должно осуществляться незамедлительно. Процедура может быть инициирована на основании мониторинга интернета, а также уведомлений от органов власти, организаций и граждан.

В 2014 году в РФ по требованию прокуратуры заблокировали более 900 экстремистских сайтов.

Президент Российской Федерации В.Путин в этом году минимум дважды обращал внимание на эти вопросы:

4 марта 2015 г. на расширенном заседании коллегии МВД Владимир Путин отметил попытки использовать так называемые «цветные технологии» — от организации незаконных уличных акций до открытой пропаганды вражды и ненависти в социальных сетях. Цель этих действий очевидна — спровоцировать гражданские конфликты, ударить по конституционным основам нашего государства, по суверенитету страны в конечном итоге.

26 марта 2015 г., выступая на заседании коллегии ФСБ Президент, среди иных вопросов обеспечения информационной без-

опасности, отметил, что в части противоправного контента было выявлено свыше 25 тысяч интернет-ресурсов с публикациями, нарушающими закон. Прекращена работа более полутора тысяч экстремистских сайтов. Президент поставил задачу продолжать очищать российское интернет-пространство от незаконных, преступных материалов, более активно использовать для этого современные технологии, участвовать в формировании системы международной информационной безопасности.

Владимир Путин отметил, что речь не идёт о том, чтобы ограничивать свободу в интернете, Необходимо строго соблюдать российские и международные правовые нормы и стандарты в данной сфере. Не препятствовать общению людей в сети и размещению там законной, допустимой и корректной информации.

Как видим, все политики озвучивают общие взгляды на проблемы распространения экстремистской идеологии через глобальные коммуникации и социальные сети. Но пока никто не предложил как выработать общие механизмы противостояния и борьбы с этим явлением.

Хочу напомнить, что проблема фильтрации контента в глобальном информационном пространстве рассматривалась в ходе работы 7-й (апрель 2013 г., Гармиш-Партенкирхен) конференции нашего Консорциума (МИКИБ). Обсуждение показало, что большинство экспертов не сомневается в необходимости фильтрации вредоносного контента — и ряд развитых государств уже применяет такую практику. Вопрос только в том, какие выбраны механизмы определения контента как вредоносного, и какие средства используют для его фильтрации.

Эксперты согласились в необходимости соблюдения баланса между правами и свободами Интернет-пользователей и обеспечением безопасности в информационной среде.

Каждое государство в рамках национального информационного пространства вправе решать какие механизмы использовать: «Отключать» или «не отключать» национальный сегмент Интернета от глобальных сетей, закрывать отдельные Интернет-ресурсы и аккаунты в социальных сетях, усиливать уголовную ответственность, принимать иные, возможно жесткие меры — это внутреннее дело каждого государства.

Так, 15 марта этого года Правительство Франции заблокировало 5 сайтов за пропаганду идей джихада. Эта мера вызвала неоднозначную реакцию: с одной стороны Правительство обвинили в нелигитимности действий, в административном подходе;

с другой стороны прозвучала критика эффективности данного решения, т.к. эти ресурсы могут изменить свои адреса или разместиться за пределами Франции.

Это подтверждает мысль о том, что только на национальном уровне решение данных проблем невозможно.

Распространение противоправного контента в социальных сетях служит не только преступным, экстремистским и террористическим целям. В ряде регионов и стран отрабатываются технологии использования глобальных сетей, социальных медиа и мобильной связи для проведения трансграничных информационно-психологических воздействий на общественное сознание, организации массовых волнений и государственных переворотов. Т.е. вмешательство во внутренние дела суверенных государств. Самый распространённый пример — события в Тунисе, Ливии и Египте.

На наш взгляд, порой в освещении в социальных сетях отдельных событий в Украине есть элементы вмешательство во внутренние дела этой страны и России.

Сложность противодействия угрозам пропаганды экстремизма и вмешательства во внутренние дела суверенных государств через социальные медиа сохраняется и углубляется. Практика свидетельствует, что только национальных регулятивных, в том числе запретительных, правовых норм для решения этих задач недостаточно. Трансграничный характер информационного пространства требует согласованных действий государств, международного сообщества. Конечно, на единых принципах равноправия, взаимного учета интересов и с опорой на международное право и соответствующие Декларации ООН.

27 сентября 2014 года, выступая на пленарном заседании 69-й сессии Генеральной Ассамблеи ООН, министр иностранных дел России Сергей Лавров предложил принять декларацию о недопустимости вмешательства во внутренние дела суверенных государств, о непризнании госпереворотов как метода смены власти. На наш взгляд, это предложение приемлемо и к цифровому пространству, к социальным сетям.

9 января 2015 г. государствами-членами ШОС в качестве официального документа ООН были внесены «Правила поведения в области обеспечения международной информационной безопасности». В документе, среди прочих предложений международному сообществу, представлены следующие:

- Не использовать ИКТ и информационные и коммуникационные сети для вмешательства во внутренние дела других государств и

в целях подрыва их политической, экономической и социальной стабильности (п. 3 Правил поведения);

- ...сдерживать распространение информации террористического, сепаратистского или экстремистского характера, а также разжигающей ненависть на национальной, расовой или религиозной почве (п. 4 Правил поведения).

На наш взгляд, эти положения заслуживают самого внимательно рассмотрения и поддержки. Было бы интересно услышать мнение наших коллег по этим предложениям.

Спасибо.

R.A.Sharyapov
Institute for Information Security Issues at MSU

Challenges of countering the threat of the use of social media for interference in the internal affairs of sovereign states

Dear Colleagues!

The topic of today's meeting — Challenges of countering the threat of the use of social media for interference in the internal affairs of sovereign states (extremism, radicalization etc.) is of utmost importance. We bring the following issues to the discussion:

1. Social media as a new phenomenon of public life: benefits and implications;
2. Use of Social media for destructive purposes: analysis and prognosis;
3. International and national mechanisms of countering the threat of interference in the internal affairs of sovereign states.

There is a stable upward trend in the role and importance of social networks, whose history began in 1995 with the introduction of an American portal Classmates.com. Any socially significant event is currently being discussed by the interested and active users of social networks.

The number of users in social networks is estimated to grow up to 2.2 billion (or 31% of the global population) in 2015, spending on advertising in social networks totaled more than $ 15.3 billion in 2014.

Social networks today not only allow socializing on various topics, exchange of opinions and acquisition of information, organization and management of business, but also are increasingly becoming targets and the means of information-psychological influence and control at different levels (regionaly, within a country, or international community). Web and social media are the essential tools of destructive information and psychological influences including for the purpose of manipulation of individuals, social groups and society as a whole.

At that I would like to mention that the problem of destructive use of the Internet and social networks, as a threat of intervention in the internal affairs, is especially relevant for countries with sufficient level of Internet penetration (according to ITU, by the end of 2014 there were nearly 3 billion Internet users, or 42.3% of the population of the planet).

Unfortunately, at the moment radicalization is a dynamic expanding process, which penetrates all social strata. And social networks are used as the main instrument of propagation.

A universally recognized growth of radicalization leads to socialization of extremism that lies in the foundation of terrorism.

The recent terrorist attacks in Europe have necessitated the revision and revitalization of action against the propagation of these ideas, and above all, through social networks.

In 2014, the «Islamic State of Iraq and Syria» (ISIS) used at least 46,000 Twitter accounts, according to The Wall Street Journal, citing a Brookings Institution report.

According to research led by the European Parliament in 2015, 90% of all terrorist activities, including propagation of radicalism and extremism, is conducted online with the use of social media.

World leaders, government officials and security chiefs have similar positions on the issue of extremist ideology propagation through social media.

In November 2014 director of the Government Communications Headquarters UK (GCHQ) Robert Hannigan wrote that the leading social media have become a convenient springboard for terrorist organizations; that ISIS terrorists have used online capabilities to create a global international terrorist network; and instant messengers and social media are used by extremists to propagate their ideas and recruit new members.

In February 2015 the Secretary of Homeland Security Jay Johnson said in a media interview that in comparison with planning and organization of the 9/11 attacks, the modern terrorist organizations are more efficiently using the Internet, social media and other means to provoke standalone attacks.

During the Summit on countering violent extremism (in February of 2015 in Washington, DC) the US President Barack Obama, the UN Secretary General Ban Ki-moon, the EU High Representative Federica Mogherini in their speeches all raised the problem of using online media and social networks to spread the ideas of extremism and terrorism, indoctrination of young people, recruiting of new members of extremist and terrorist groups, and propagation of the virus of fear.

At conclusion of the Summit (and it brought together government representatives from more than 60 countries, including the director of Federal Security Service of the Russian Federation A.V.Bortnikov), there has been made a joint statement in which one of the proposed measures involved the use of global communications, including social media, to counter aggressive extremist messages.

Let me remind you that at the meeting of our Forum yesterday Bruce McConnell, talking about the priorities of the East-West Institute, placed the issue of destructive content into second place.

Countering the spread of the ideology of extremism and radicalism through social media is relevant in Russia as well.

On February 1, 2014 in a new law came into force in Russia allowing the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) at request of the General Prosecutor to block resources with calls for extremism and riots without trial. Restriction of access to such sites should be carried out immediately. The procedure can be initiated on the basis of Internet monitoring, as well as notifications from authorities, organizations and citizens.

In 2014, more than 900 extremist websites have been blocked in the Russian Federation at request of the public prosecution office.

The President of the Russian Federation Vladimir Putin, drew attention to these issues at least twice this year:

On March 4, 2015 at the enlarged meeting of the collegium of the Ministry of Internal Affairs Vladimir Putin mentioned the attempts to use the so-called «color technologies» —from organization of illegal street protests to outright propaganda of enmity and hatred in social media. The purpose of these actions is obvious — to provoke civil strife, damage the constitutional foundations of our country, and eventually its sovereignty.

On March 26, 2015, upon addressing the meeting of the collegium of the Federal Security Service of the Russian Federation, the President mentioned, among other issues of information security, that with regard to illegal content more than 25 thousand online resources were ruled to violate the law. More than one and a half thousand extremist websites have been shut down. The President has set a task to continue to clear the Russian Internet space from illegal, criminal content, to this end actively use modern technologies, and to participate in the development of an international information security system.

Vladimir Putin noted that this is not about restriction of freedom on the Internet. In this area it is necessary to comply with Russian and international law and standards and not to obstruct the communication between individuals and publication of legitimate, appropriate and correct information.

As you can see, all politicians express similar views on the problems of dissemination of extremist ideology through global communication and social media. But so far no one has proposed a way to develop common framework of countering and fighting this phenomenon.

I would like to bring to mind that issues of content filtration in the global information space have been discussed in the course of the VII Conference of our Consortium (IISRC) in April 2013, Garmisch-Partenkirchen. The discussion showed that most experts do not doubt the need for filtering of objectionable content — and a number of developed countries have already implemented this practice. The only question is what mechanisms are in place for identification of objectionable content, and what means are used for its filtration.

Experts agreed with the need to find the balance between the rights and freedoms of Internet users and security of information space.

Each country has the right to decide what frameworks should be used in national information space. It is an internal matter for each country whether to «disconnect» the national segment of the Internet or remain «connected» to the global networks, to shut down certain Internet resources and accounts in social media, strengthen criminal responsibility, or implement other, possibly tougher measures.

For example, on March, 15 of this year, the government of France blocked five websites for propagation of the ideas of jihad. This measure spawned controversy: on the one hand the government was accused of illegitimacy of actions and of administrative approach; on the other hand there was criticism of the effectiveness of this measure, as these resources can change their addresses or be hosted outside of France.

This confirms the notion that it is impossible to solve these problems only on a national level.

The dissemination of illegal content in social media serves not only criminal, extremist and terrorist purposes. In a number of regions and countries, there is an ongoing testing of technologies of using global networks, social media and mobile communication for cross-border information and psychological influence on public consciousness, organization of mass unrest and coups — i.e. interference in the internal affairs of sovereign states. The most common examples are the events in Tunisia, Libya and Egypt.

In our opinion, in social media coverage of a detached events in Ukraine, there are at times attributes of intervention in the internal affairs of this country and Russia.

The complexity of countering the threats of extremism propaganda and interference in the internal affairs of sovereign states through social media remains unchanged and is deepened. Practice shows that national regulatory (including prohibitive) norms alone are not enough for solution of these problems. The transboundary nature of information space necessitates concerted action of nation-states and international community. This action should be based, of course, on common

principles of equality and mutual interests and on international law and the relevant United Nations declarations.

On September 27, 2014, speaking at the plenary session of the 69th session of the UN General Assembly, Russian Foreign Minister Sergei Lavrov proposed to adopt a declaration on prohibition of interference in the internal affairs of sovereign states and non-recognition of coups as a method of shift of power. In our opinion, this proposal is applicable to information space, to social media.

On January 9, 2015 the SCO member-states have submitted to the United Nations an «International code of conduct for information security». The document, among other proposals to international community, includes the following:

- Not to use information and communications technologies and information and communications networks to interfere in the internal affairs of other States or with the aim of undermining their political, economic and social stability (Article 3);
- ...curbing the dissemination of information that incites terrorism, separatism or extremism or that inflames hatred on ethnic, racial or religious grounds (Article 4).
- In our view, these provisions deserve careful consideration and support. It would be interesting to hear the opinion of our colleagues on these proposals.

Thank you.

Кеир Гилс

Центр исследования конфликтов (Великобритания)

Осознание Западом серьёзности информационного противоборства

Введение

Предыдущие выступления автора на этой и других конференциях зачастую выполняли посредническую роль: либо объясняли российские взгляды на информационную безопасность западной аудитории, или, наоборот, объясняли российской аудитории, как эти взгляды интерпретируются за рубежом[1]. Одним из постоянных аспектов было обсуждение и объяснение того, каким образом в российской политике информационной безопасности находит выражение целостный подход к противодействию информационным угрозам, в частности, выделение проблемы вредоносного контента, а также отдельная «кибер» угроза вредоносного кода.

Западные теоретики и политики, занимающиеся вопросами кибербезопасности, напротив, до недавнего времени были по большей части невосприимчивы к понятию вредоносного контента. Представление о том, что свободное выражение мнения или точки зрения может нести в себе опасность, воспринималось как нечто экзотическое и дикое, и *априори* отвергалось, в то время как свобода выражения мнений и свободное перемещение информации через границы оставались неприкосновенными. В настоящее время это основное допущение изменилось до неузнаваемости по причине двух обособленных проблем, которые стоят перед Западным обществом: российское информационное противоборство, сосредоточенное на украинском конфликте; и исламское государство (далее ИГИЛ) со своими специфическими целями.

Исследования этих двух проблем на Западе показывают, что они имеют некоторые схожие черты, но в то же время отличаются по существу: в действительности же, значительная часть дискуссии посвящена тому, какая из двух проблем представляет собой более

[1] См. Кеир Гилс, «Взгляд через кривое зеркало: российские интересы в сфере информационной безопасности в представлении зарубежных государств», материалы Седьмого международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности», Гармиш-Паренкирхен, Германия, Апрель 2013, стр. 238–245.

актуальную угрозу Западу, Россия или ИГИЛ.[2] И в том, и в другом случае ключевым элементом проблемы является «многоуровневый процесс, связанный с электронными СМИ, в ходе которого некоторое количество производственных единиц... создает контент в соответствии с основной... идеей»[3]. В результате впервые за многие десятилетия Запад был вынужден рассматривать либеральные принципы свободы выражения мнений в контексте их практического применения — не на основе идеализма, а в ходе противодействия реальной и непосредственной проблеме.

Что касается кибербезопасности, конфликт в Украине, в частности, способен оказать трансформирующий эффект на кибердоктрину. В отличие от России, изолированный подход Запада к кибербезопасности, как правило, опирается на технические решения технических угроз, и в значительной степени игнорирует связь с информационной войной в широком смысле. Это полностью подходит для противодействия долговременным или фоновым угрозам, но, скорее всего, этого будет недостаточно в кризисных ситуациях, так как в тот момент не будет такого понятия, как «чистое кибер противостояние». Иными словами, Запад, возможно, хорошо подготовился к кибервойне, но, как показывают события в Украине, он также должен быть готов к информационной войне, в которой кибероперации выполняют вспомогательную роль.

Ранее исключения из этого правила были найдены в специализированных областях военной науки, связанных с информационной войной. Речь идёт об исследованиях, которые ограничиваются только военными операциями (хотя и здесь множество предостережений и оговорок, применяемых отдельными странами к доктрине НАТО, говорит о значительной противоречивости вопроса);[4] и о недавних исследованиях по изучению использования социальных медиа для оказания воздействия, вплоть до смены режима (хотя даже во время Арабской весны, на Западе этому вопросу уделял внимание лишь узкий круг специалистов)[5]. Но недавние собы-

---

[2] «NATO and New Ways of Warfare: Defeating Hybrid Threats», NDC Conference Report, NATO Defense College No. 03/15, Военный колледж НАТО, Рим, Май 2015.

[3] «Violent Islamist Extremism, The Internet, and the Homegrown Terrorist Threat», Комитет Сената США по вопросам Внутренней безопасности и государственным делам, 8 Мая 2008, http://www.hsgac.senate.gov//imo/media/doc/IslamistReport.pdf

[4] См публикацию НАТО AJP-3.10, «Allied Joint Doctrine For Information Operations».

[5] См., например, Scott Railton, «Revolutionary Risk-Cyber Technology and Threats in the 2011 Libyan Revolution», US Naval War College, 2013.

тия вызвали более глубокий сдвиг концептуальных представлений об информационной угрозе у западных СМИ, правящих кругов и общества. Возникло в значительной степени новое представление об информационных угрозах, которое воплотило в себе признание того, что проблемы и угрозы несет как вредоносный код, так и враждебная информация в виде контента. Ирония заключается в том, что это, по сути, движение в сторону российской точки зрения на информационную безопасность.

Уязвимости

Информационные кампании и России, и ИГИЛ направлены точно на внутренние недостатки западных либерально-демократических обществ, и используют широкий спектр самопричиненных уязвимостей, которые имеют основополагающее значение для самоопределения этих обществ и их ценностей.

К ним относятся:

- Догматическая преданность свободе выражения как Абсолюту;
- Мощные либеральные СМИ, со своим иногда специфическим пониманием того, что служит интересам национальной безопасности;
- В тех же СМИ есть приоритет баланса над объективностью;
- Тенденции в сфере пользовательского контента за последние 15 лет, в том числе повсеместное распространение платформ для читателей и слушателей для добавления собственных комментариев к репортажам СМИ;
- Политические лидеры получают в основном те же потоки информации, что и их электорат, и таким же образом воспринимают их.

Каждая из этих уязвимостей представляет собой отдельный вектор атаки для тех, чьей целью является манипуляция информацией для достижения социального или политического эффекта. И в каждом случае социальные медиа играют роль — как канала доступа, так и операционной среды. Оба актора получают выгоду от запоздалого признания того, что «цифровые СМИ становятся главными — а для возрастающего числа молодых людей — и единственными каналами политической информации и коммуникации. Они являются основным пространством политической деятельности, где граждане получают политическую информацию, формируют свои политические взгляды и убеждения, и имеют возможность влиять на процессы, связанные с функ-

ционированием власти»[6] — и, как следствие, «новые социальные медиа стали наиболее эффективным инструментом для воздействия на умы огромных сообществ, и даже целых народов»[7].

В российском случае, кибердеятельность в широком смысле имеет решающее значение для наступательных дезинформационных кампаний, будь то создание поддельных Интернет-СМИ[8] для распространения дезинформации, или использование социальных медиа для подрывной и дестабилизирующей деятельности против внеплановых целей, по-видимому, не связанных с событиями в Украине[9]. Эти мероприятия дополняются вездесущей деятельностью троллей и ботов, которые используют особенности отношений между традиционными и социальными медиа для внедрения, распространения и повышения доверия к дезинформации[10]. Для достижения нужного эффекта они используют ряд других мер, например, замалчивание пропагандистскими СМИ своей аффилированности, чтобы приманить зрителей в Соединенных Штатах и других странах[11], установление связей с крайне правыми политическими партиями для накопления прямого политического влияния[12], и подрывные мероприятия старой школы, такие как «дипломатия НПО, или создание и поддержка за рубежом пророссийских молодежных групп, меньшинств, сепаратистских организаций и исследовательских центров»[13]. В результате на внешнем уровне множественные ложные сведения, продвигаемые в ходе российских информационных кампаний, попадают

---

[6] Velichka Milina, «Security in a Communications Society: Opportunities and Challenges», Connections, Spring 2012, Volume XI, Number 2, p. 55.

[7] *Ibid.*

[8] Dalibor Rohac, «Cranks, Trolls, and Useful Idiots: Russia's information warriors set their sights on Central Europe», Foreign Policy, 12 March 2015, https://foreignpolicy.com/2015/03/12/cranks-trolls-and-useful-idiots-poland-czech-republic-slovakia-russia-ukraine/

[9] Doug Bernard, «America's Adversaries Use Baltimore Unrest to Spread Anti-US Message», VOA News, 30 April 2015, http://www.voanews.com/articleprintview/2743166.html

[10] Polina Tikhonova, «Russia Hacking Your News», ValueWalk, 14 March 2015, http://www.valuewalk.com/2015/03/russia-hacking-your-news/

[11] Jill Dougherty, «Russian TV's American Face», Huffington Post, 4 November 2014.

[12] «"Черный интернационал". Как Москва кормит правые партии по всему миру», The Insider, 27 November 2014, http://theins.ru/politika/2113. См. также Andrew Higgins, «Waving Cash, Putin Sows E.U. Divisions in an Effort to Break Sanctions», New York Times, 6 April 2015, http://nyti.ms/1ac5osT

[13] Sinikukka Saari, «Russia's public diplomacy: soft tools with a hard edge», Border Crossing (Diplomat Magazine), April 2015.

на благодатную почву среди населения, которое не очень хорошо информировано о реалиях истории, географии, и о том, что поставлено на карту в Украине.

Эти группы населения, и, в частности, их свободные СМИ, в начале 2014 года оказались совершенно неподготовленными к противодействию натиску скоординированной информационной войны[14]. Западные общества верят, что их независимые СМИ найдут и покажут истину благодаря своей относительной свободе действий. Но подготовка западных либеральных СМИ изначально не могла противостоять единству сообщений, исходящих из России. На самом деле было верно обратное: акцент на сбалансированной подаче материала во многих западных СМИ привел к тому, что враждебные сообщения, какими бы заведомо ложными они не являлись, были повторены европейским и американским зрителям их СМИ. Шла ли речь о преувеличении ИГИЛ своей мощи и охвата, или о широком спектре сообщений в поддержку российской общественной дипломатии, необходимость баланса привела к тому, что новостные редакторы жестко следовали тезису, что у каждой истории должно быть две стороны — даже если на самом деле была только одна[15]. Следовательно, даже если западным новостным редакторам давалась заведомо ложная информация, у них не было другого выбора, кроме как сообщить её — значит придать ей вес и авторитет.

Интернет и социальные СМИ также сыграли здесь свою определенную роль. В российском случае, армия троллей Кремля взаимодействовала непосредственно с читателями на различных площадках, включая форумы, Twitter и др., выступая в качестве мультипликатора силы для внедрения в сознание российских взглядов — особенно перенаправляя или подавляя любую дискуссию, которая обращала внимание на несоответствия или неправдоподобность российской версии событий. В результате совокупность масштабов, интенсивности, объема и последовательности российской аргументации в сети, вместе с повторением последовательной версии событий на всех уровнях российской медиа-машины от президента до рядового в армии троллей Кремля, продолжает использовать проблему приоритета баланса

---

[14] Nick Cohen, «Russia Today: why western cynics lap up Putin's TV poison», The Observer, 8 November 2014, http://www.theguardian.com/commentisfree/2014/nov/08/russia-today-western-cynics-lap-up-putins-tv-poison

[15] Рассматривается в норвежском контексте Кжелем Драгенсом (Kjell Dragnes) в «Journalister i propagandaens tid», Aftenposten, 23 March 2015, http://www.aftenposten.no/meninger/Journalister-i-propagandaens-tid-7954103.html

над объективностью западных СМИ и может привести к тому, что освещение событий и дальше будет испорчено принятием во внимание полностью ложных, но вездесущих, российских альтернативных сообщений.

Таким образом, западные СМИ показали себя полностью неготовыми противостоять скоординированной и хорошо обеспеченной ресурсами информационной кампании. Вначале это привело к поразительно успешному внедрению сообщений, которые в значительной степени способствовали возможности России проводить операции против Украины на ранних стадиях конфликта в условиях слабо согласованного противостояния со стороны Запада. Тот факт, что в течение практически года ЕС был не в состоянии публично высказываться о присутствии российских войск в Украине[16], означает полную неспособность оспорить русскую версию событий — без чего невозможен осмысленный ответ. Раннее освещение конфликта СМИ показало «очевидность того, что некоторые собеседники полностью поверили в некоторые грубые подделки российской пропаганды»[17].

По сравнению с доинтернетовской эпохой, эффективное внедрение этих фальсификаций значительно упростилось. Имели место такие привлекающие внимание грубые методы, как взлом ленты Твиттера крупного информационного агентства для внедрения дезинформации[18], но даже они совершенно не нужны, когда сообщения могут быть введены в СМИ с помощью других, казалось бы, естественных и законных средств. Основные коммерческие новостные СМИ в западных странах значительно сократили персонал ввиду того, что доходы от рекламы перешли к другим СМИ, и лишь немногие из множества возникших любительских блогов и форумов имеют возможности для самостоятельной серьезной проверки источника. Следовательно, марионеточные сайты, которые производят впечатление сообщающих или агрегирующих новости, могут добиться существенного охвата и проникновения. После того, как размещенная там дезинформация попадает в основную новостную ленту в одной или

---

[16] Andrew Rettman, «EU breaks taboo on 'Russian forces in Ukraine'», EU Observer, 16 February 2015, https://euobserver.com/foreign/127667

[17] John Besemeres, «Russian disinformation and Western misconceptions», Inside Story, 23 September 2014, http://insidestory.org.au/russian-disinformation-and-western-misconceptions

[18] «AP Twitter hack causes panic on Wall Street and sends Dow plunging», The Guardian, 23 April 2013, http://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall

нескольких точках, и подхватывается и сообщается авторитетными традиционными СМИ, чьи редакторы и журналисты не поняли, что это дезинформация, другие следуют за ними: даже в новой обстановке осведомленности основные средства массовой информации не хотят игнорировать события, которые оказались в новостной повестке дня.

Отрицание

По мере того, как осознание природы российской информационной кампании начало просачиваться через западные СМИ и круги, принимающие политические решения, это привело к опасному оптимизму по поводу эффективности российских мер и широкому распространению мнения, что российская дезинформация не работает из-за отсутствия правдоподобности[19]. Предположительно, российские вымыслы и опровержения были неэффективны, потому что они были настолько очевидны, что они не подействовали на высокопоставленных или думающих индивидов на Западе. Этот аргумент был соблазнительным: по западным меркам, значительная часть российской дезинформации кажется неуклюжей, контрпродуктивной, очевидной и легко опровергаемой. Но оценка кампании по этим стандартам несла в себе значительный риск неверной интерпретации российских целей. В частности, сначала она привела к недооценке последствий наслаивания сообщений, когда более тонкая агитация экранировалась и маскировалась очевидной пропагандой устойчивой интенсивности, и пагубного влияния «пузыря фильтрации» на привычки онлайн-чтения. Она также не смогла учесть изначально отсутствовавшую осведомленность о дезинформации и враждебной пропаганде, распространяемой не только на европейских языках, но также на арабском и русском — нацеленной на меньшинства в европейских государствах.

Напротив, измеренная по российским меркам, информационная кампания, по сути, добилась значительных успехов. Это особенно относится к двум ключевым направлениям: внутреннему, по контролю отечественной сферы средств массовой информации; и внешнему, по влиянию на массовое сознание, и созданию среды, в которой трудно выделить качественную ин-

[19] Например, как говорит проф. Лоуренс Фридман: «попытки ввести в заблуждение были по большей части неэффективны, поскольку роль России начала проясняться». Lawrence Freedman, «Ukraine and the Art of Limited War», Survival: Global Politics and Strategy, 56:6, 7-38 (2014).

формацию, для того, чтобы подорвать объективность репортажей западных СМИ и, следовательно, повлиять на информацию, доступную политикам (старший корреспондент уважаемой британской национальной газеты в апреле 2015 года всё еще говорил, что большое число писем и комментариев и ответов через социальные медиа в поддержку политики России отражает широкую общественную поддержку среди читателей). Вместе они образуют комбинированную оборонительную и наступательную стратегию, работающую через внутренние и внешние СМИ[20].

Реакция — Правительство

В сентябре 2011 года в подробном отчете, представленном британским исследовательским центром Chatham House, были определены направления для существенного улучшения политики информационного обеспечения и её реализации западными правительствами — даже до того, как эти правительства были подвергнуты текущему стресс-тесту в виде длительной информационной кампании.[21] А на правительственном и наднациональном уровне окончательная форма общей реакции на новую угрозу информационной войны остается неясной и на момент написания. Обсуждение информационной войны как проблемы было включено в обсуждение «новых» форм войны в целом — называемых иррегулярными, нелинейными, асимметричными или гибридными. Но уже появились некоторые отдельные темы, касающиеся мер реагирования, не рассматриваемых западными правительствами. Представляется, что четыре различных тактики защиты от информационной войны уже были отброшены.

1. *Не будет никаких ограничений свободы выражения мнений и никакого управления СМИ.*

В тех редких случаях, когда этот подход вообще поднимался в обсуждении, как представляется, он немедленно и категорически отвергался. Контроль над контентом или цензура мнений — неважно, собственное ли это мнение, или проплаченное — не является вариантом для западных либеральных демократий. Правящие круги в этих обществах по-прежнему поддерживают либеральные ценности и отвергают любое копирование российских мер по контролю внутреннего общественного мнения. Они

---

[20] Matthew Armstrong, «Russia's War on Information», War on the Rocks, December 2014, http://warontherocks.com/2014/12/russias-war-on-information/

[21] Paul Cornish, Julian Lindley-French and Claire Yorke, «Strategic Communications and National Strategy», Chatham House report, September 2011.

следуют принципу, выдвинутому в 1946 году американским дипломатом Джорджем Кеннаном, что «самая большая опасность, которая грозит нам в решении этой проблемы... это уподобление тем, с кем мы имеем дело»[22].

2. *Не будет симметричного ответа на гибридные кампании. В частности, западные правительства не будут участвовать в систематических кампаниях по дезинформации*[23].

Множественная противоречивая неправда является ключевым элементом российского подхода к информационной войне. Но западные лидеры, привлекаемые к ответственности либеральными СМИ и критически мыслящими сообществами, знают, что любая ложь недолговечна и контрпродуктивна. Их единственным вариантом ответа является четкое следование истине.

3. *Не будет введено понятия национального информационного пространства и, следовательно, понятия «нарушений» в этом пространстве, как описано в российской доктрине информационной безопасности.*

По-прежнему воспринимается как должное, что Интернет по самой своей природе зависит от свободного и беспрепятственного прохождения информации через национальные границы, и не было никаких предложений по ограничению этого.

4. *Пока что нет видимых шагов к созданию в правительстве национальных органов по оборонительному информационному обеспечению — другими словами, органов противодействия информационной войне.*

Некоторые ограниченные шаги по внедрению комплексного подхода к информационной войне можно наблюдать в военной среде, например, с созданием 77 бригады ВС Великобритании, объединившей ряд различных подразделений, действующих в различных информационных мероприятиях. Но в целом задачи отслеживания и противодействия дезинформации по-прежнему главным образом возложены на такие добровольческие и неправительственные организации как Bellingcat[24], the Interpreter[25] или Stopfake[26], без очевидного правительственного или международного участия.

---

[22] «Длинная телеграмма», Дж. Кеннана Дж. Маршаллу, 22 февраля 1946, доступно по адресу (англ.): https://www.trumanlibrary.org/whistlestop/study_collections/coldwar/documents/pdf/6-6.pdf

[23] «Ümarlaud: Vene propaganda vastu võitlemise asemel tuleb pakkuda alternatiivi», Postimees, 18 February 2015, http://www.postimees.ee/3096321/umarlaud-vene-propaganda-vastu-voitlemise-asemel-tuleb-pakkuda-alternatiivi

[24] https://www.bellingcat.com/tag/russia/

[25] http://www.interpretermag.com/about-us/

[26] http://www.stopfake.org/en/news/

В других областях рассеянная, несогласованная и саморегулирующаяся природа социальных медиа способствовала возникновению эффективных механизмов самозащиты. Готовность к широкому распространению организованных троллями кампаний привела к тиражированию руководств самопомощи для противодействия троллям в отсутствие модераторов[27], а увеличение доступности инструментов для обнаружения кампаний троллей и ботов помогает повысить осведомленность[28]. В результате этого, согласно одному российскому исследованию, несмотря на «миллиарды долларов», потраченных Россией в попытке «превратить социальные сети в своё послушное оружие», «сетевое сообщество выработало иммунитет. Теперь отрицательный эффект от попыток Кремля манипулировать мнением сетевого общества таков, что фактически сводит на нет эти усилия»[29].

Осознание деструктивного потенциала враждебных информационных кампаний возрастает также в областях, которые абсолютно не связаны с государственными или негосударственными противниками, такими как Россия или ИГИЛ. В науке отмечается феномен распространения источников, который подрывает доверие к авторитетным изданиям. Проблема заключается в «хищнических журналах», которые разбавляют правильно рецензируемые научные статьи непроверенным материалом, что приводит к тому, что читатели «не в состоянии отличить заслуживающие доверия исследования от лженауки»[30]. А в Великобритании споры по поводу местных выборов в лондонском районе Tower Hamlets привлекли широкое внимание к уязвимости либеральных политических процессов к подрывным информационным кампаниям. Этот инцидент продемонстрировал, как специализированная группа лиц способна захватить политическую власть с помощью совместных усилий, направленных на точки восприимчивости конкретного сообщества, с помощью запугивания, дезинформа-

---

[27] Главным примером является популярная инфографика, на которой изображены «Пять этапов спора с российским националистом», доступно по адресу: http://i.imgur.com/ka4Gmd0.jpg

[28] Lawrence Alexander, «A Response to the KremlinBot Skeptics», Global Voices, 24 April 2015, http://globalvoicesonline.org/2015/04/24/a-response-to-the-kremlin-bot-skeptics/print/

[29] «Владимир Голышев: «В информационной войне надо «идти на грозу»»», Russkiy Monitor, 29 January 2015, http://rusmonitor.com/vladimir-golyshev-v-informacionnojj-vojjne-nado-idti-na-grozu.html

[30] Robert E Bartholomew, «Science for sale: the rise of predatory journals», Journal of the Royal Society of Medicine: 2014, Vol. 107(10), pp. 384–5.

ции, использования культурных и религиозных уязвимостей, и работы с недовольными — используя существующее или искусственное чувство обиды или отстраненности[31].

В конце 2014 года западные СМИ продолжали добросовестно повторять российскую дезинформацию как факт, но в репортажи начало просачиваться осознание того, что они стали жертвами согласованной подрывной кампании. В традиционных СМИ (в том числе их онлайн-версиях) это проявилось в закрытии или модерировании ранее открытых форумов и отказ от пользовательского контента. Под угрозой скоординированных действий троллей также были удалены ссылки на социальные медиа. Как это ни парадоксально, одним из первых крупных новостных агентств, предпринявших эти шаги, был *The Guardian* в Великобритании — ранее оплот либерального экстремизма и свободы выражения мнений, вплоть до того, что в разгар событий, связанных со Сноуденом, его редакторы считали себя самопровозглашенными арбитрами и сами решали, отвечала ли публикация похищенной секретной информации национальным интересам[32].

Но признание отдельными СМИ, что их объективность и независимость были подорваны российскими кампаниями дезинформации и троллинга[33], в целом не привело к скоординированной реакции. В частности, необходимость «сбалансированной подачи информации» по-прежнему представляет собой ключевую проблему. В результате этого требования, даже статья уважаемого дипломатического корреспондента, объясняющая природу «гибридной войны» (широко принятый на Западе термин, которым обозначают природу российских кампаний в Украине и за её пределами), включает в себя шесть параграфов с российскими опровержениями, утверждающими, что вся эта концепция сфабрикована Западом для дискредитации России[34].

---

[31] "Judgment In The High Court Of Justice, Queen's Bench Division, In The Matter Of The Representation Of The People Act 1983 And In The Matter Of A Mayoral Election For The London Borough Of Tower Hamlets Held On 22 May 2014", доступно по адресу: http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/judgment.pdf

[32] Кеир Гилс, «Легитимизация онлайн-слежки и мониторинга», материалы Восьмого международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности», Гармиш-Паренкирхен, Германия, Апрель 2014

[33] Chris Elliot, «The readers' editor on... pro-Russia trolling below the line on Ukraine stories», The Guardian (May 4, 2014), http://www. theguardian.com/commentisfree/2014/may/04/pro-russia-trolls-ukraine-guardian-online

[34] Bridget Kendall, «Hybrid warfare: The new conflict between East and West», BBC News, 6 November 2014, http://www.bbc.co.uk/news/world-europe-29903395

Национальные международные вещательные компании на Западе столкнулись с другой проблемой. Deutsche Welle, Всемирной службе BBC, Радио Свободная Европа и другим было поручено выйти на российскую аудиторию для противодействия альтернативной реальности, существующей в российском медиапространстве, с особым упором на российские боевые операции в Украине. Для западных военных медиасознание является неотъемлемой частью оперативного планирования. Это связано с признанием того, что распространение СМИ и средств мгновенной связи «позволяет гражданам тщательно изучать то, как вооруженные силы их страны ведут войны ... [что приводит к] возможности непосредственного влияния общественного мнения на принятие политических решений»[35]. Но в 2015 году это является асимметричной уязвимостью, так как это применимо к западным либеральным демократиям со свободными СМИ, но, как убедительно продемонстрировали события вокруг Украины, не к России.

Вместо этого, Россия предприняла ряд эффективных мер, чтобы оградить себя от такого контроля со стороны собственного населения. Эти меры включают в себя способы изоляции россиян от внешних источников информации — устанавливаются как явные, так и скрытые элементы системы, которую Даниэль Шеарф, руководитель московского бюро Голоса Америки, описывает, как новый «железный занавес для СМИ»[36]. Это приводит к тому, что на внутреннем информационном пространстве полностью доминируют государственные СМИ, и задолго до событий на Украине осуществлялось централизованное управление повесткой дня[37]. Результатом является неузнаваемая российская альтернативная реальность[38], в которой «российские СМИ за редким исключением отказались, иногда через принуждение, но в основном добровольно и даже охотно, от функции информирования общественности и превратились в создателей Матрицы — искусственной реальности, где мнимые герои и злодеи изо всех сил сражаются

---

[35] Sanu Kainikara, «Air Power in the Information Age: The Deciding Factor», Air Power Development Centre [Australia], February 2015, p. 3.

[36] Из разговора с автором, Август 2015.

[37] Stephen Castle, «A Russian TV Insider Describes a Modern Propaganda Machine», New York Times, 13 February 2015, http://nyti.ms/1zcDqDq

[38] Gary Shteyngart, «Out of My Mouth Comes Unimpeachable Manly Truth», New York Times, 18 February 2015, http://www.nytimes.com/2015/02/22/magazine/out-of-my-mouth-comes-unimpeachable-manly-truth.html?emc=eta1&_r=0

в российском Армагеддоне»[39]. Остатки свободных СМИ в России в значительной степени подверглись маргинализации, или их заставили подчиняться[40]. Как следствие, правительства оказывают давление на свои государственные вещательные компании, чтобы те «что-то сделали» для выполнения своей задачи по донесению внешней реальности до российской аудитории.

При этом они сталкиваются с новыми проблемами. Во время холодной войны, когда эти вещатели выполняли подобные функции, основным методом передачи были короткие радиоволны. Но сегодня, даже если бы у потенциальных слушателей еще были приемники коротких волн, стоимость и сложность восстановления возможности такого вещания сделало бы его невозможным. Между тем, лицензии на ретрансляцию, которые были выпущены в России в более ранний период свободного сотрудничества со СМИ и которые позволяли вести иностранное вещание в крупных городах в FM-диапазоне, были отменены или не обновлены. В 2015 году мысль, что зарубежным вещательным компаниям будет разрешен такой же доступ на российский медиа-рынок, какой есть у Russia Today на западный, кажется невероятной[41]: в частности, потому, что доктрина России рассматривает любой такой доступ, который даёт версию событий, альтернативную официальной государственной, как однозначно враждебный[42].

Прогноз

В 2015 году отношение Запада к информационным кампаниям, обеспечившим будущие активные действия России в Восточной Европе, определялось тревогой о потенциальных последствиях информационной изоляции самой России. Для большей части российского населения, даже тех, кто проявляет осознанный интерес к внешним событиям, доступ к внешней реальности становится все более сложной задачей. Такие порталы, как ИноСМИ,

[39] Vasily Gatov, «How the Kremlin and the Media Ended Up in Bed Together», The Moscow Times, 11 March 2015, http://www.themoscowtimes.com/opinion/article/how-the-kremlin-and-the-media-ended-up-in-bed-together/517323.html

[40] Andrei Malgin, «Russia's State Media Get Away With Murder,» The Moscow Times, 4 November 2014, http://www.themoscowtimes.com/opinion/article/russia-s-state-media-get-away-with-murder/510619.html. See also «Russian media firms: Interesting news», The Economist, 8 November 2014, http://www.economist.com/node/21631057/print

[41] Keir Giles, «The information war: how Moscow controls access to Western media», The World Today, August-September 2015, p. 19.

[42] Vyacheslav Nechayev, «США вводят информационные войска в российские социальные сети», Izvestiya, 14 April 2015, http://izvestia.ru/news/585366

создают видимость окна во внешний мир, но на самом деле выборочно переводят и искажают сообщения СМИ для того, чтобы поддержать официальную российскую версию событий, изменяя и создавая мировоззрение, которое неотличимо от оригинала[43].

Существование этого фундаментального несоответствия между восприятием в России и реальностью за её пределами приводит к существенным опасностям. Среди них укрепление восприятия, что независимые государства бывшего Советского Союза, в том числе Украина и страны Балтии, в сущности, принадлежат России: как говорится в комментарии президента Путина, в 1991 году «Россия добровольно — я подчеркиваю — добровольно и сознательно сделала беспрецедентные исторические уступки, отдав свою собственную территорию»[44].

В некоторых частях российского общества эти устремления России по восстановлению имперского господства над своими прилегающими территориями всегда пользовались широкой поддержкой — Генеральный прокурор Крыма, ныне знаменитая Наталья Поклонская, в своём интервью во время аннексии заявила о своём желании «начать заново в великом государстве, великой державе, *империи*, какой является Россия»[45]. Но нынешние информационные кампании создают благоприятную почву для возникновения риторики конфронтации, которая опасна сама по себе. Интенсивная милитаризация — о которой иногда непосредственно говорят как о мобилизации — извне выглядит как пронизывающая российское общество, беспрестанно подогреваемая идущей сверху риторикой войны, противостояния и угрозы, со сплошным охватом военных передач на телевидении. Государственная интерпретация войны «манипулирует населением и настраивает его сознание на военный лад» — не только используя традиционный сюжет российской жертвенности на протяжении веков, но и вызывая «чувство героизма, что сейчас опасное время»[46]. К вящему недоумению Запада, руководство России за-

---

[43] Rolf Fredheim, «Filtering Foreign Media Content» How Russian News Agencies Repurpose Western News Reporting», Journal of Soviet and Post-Soviet Politics and Society, Vol. 1, No. 1 (2015), pp. 37–83.

[44] Ksenia Kirillova, «Путин фактически назвал Украину территорией России», Novyy Region 2, 28 April 2015, http://nr2.com.ua/blogs/Ksenija_Kirillova/Putin-fakticheski-nazval-Ukrainu-territoriey-Rossii-95566.html

[45] Интервью российскому телевидению доступно по адресу: https://www.youtube.com/watch?v=XX4JCQViRKg (at 2'40").

[46] Выступление посла Эстонии в России Юри Луйка на конференции Lennart Meri, Таллинн, 24 Апреля 2015

является, что «американцы пытаются втянуть Российскую Федерацию в межгосударственный военный конфликт, произвести смену власти под предлогом событий в Украине, и, в конечном счете, расчленить нашу страну»[47].

Наиболее опасным, как показывает анализ российского видения безопасности, является не только эта асимметрия восприятия угрозы, но и полное расхождение с Западом в плане понимания того, как и когда для борьбы с этими угрозами должна быть использована военная сила. Особенно опасным примером является новый акцент в заявлениях президента Путина и других должностных лиц о возможности применения ядерного оружия[48]. В дополнение к особой роли, которую ядерное оружие играет в российской национальной идентичности[49], представляется, что в настоящее время использование стратегических и тактических ядерных вооружений подаётся для российского внутреннего потребления как «реальная возможность»[50]. Это приводит к опасному немыслимому расхождению[51] — на Западе, который отошел от концепции времен холодной войны о ядерной угрозе между крупными державами, эти сообщения принимаются, но остаются непонятыми. Нет более хорошей мотивации для западных СМИ, обществ и правительств, чтобы приложить максимум усилий для понимания и адаптации к новым условиям информационного противоборства.

---

[47] Интервью с Секретарем Совета безопасности Российской Федерации Н.П.Патрушевым, Российская газета, 11 Февраля 2015.

[48] Tom Nichols, «If Putin goes nuclear», The War Room, 1 September 2014, http://tomnichols.net/blog/2014/09/01/if-putin-goes-nuclear/

[49] Tom Parfitt, «Ukraine Crisis: Putin's Nuclear Threats are a Struggle for Pride and Status», Daily Telegraph, 29 August 2014, http://www.telegraph.co.uk/news/worldnews/europe/russia/11064978/Ukraine-crisis-Putins-nuclear-threats-are-a- struggle-for-pride-and-status.html. Более подробное исследование: Keir Giles and Andrew Monaghan, «European Missile Defense and Russia», U.S. Army War College Strategic Studies Institute, July 2014, http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1219.

[50] Stephen Ennis, «Russian media learn to love the bomb», BBC News, 23 February 2015, http://www.bbc.co.uk/news/world-europe-31557254.

[51] Alexander Golts, «Russia's Nuclear Euphoria Ignores Reality», Moscow Times, 6 October 2014, http://www.themoscowtimes.com/advertorials/ opinion/Russia-s-Nuclear-Euphoria-Ignores-Reality/

Keir Giles
Conflict Studies Research Centre (UK)

The West Wakes Up To Information Confrontation

Introduction

This author's previous contributions to this and other conference series have frequently filled an intermediary role: explaining the Russian view of information security to Western audiences, or conversely, explaining to a Russian audience how that view is interpreted abroad[1]. One consistent element of this has been discussion and explanation of the manner in which Russian information security policy expresses a holistic approach to countering information threats, in particular recognising the problem of harmful content as well as the strict «cyber» issue of harmful code.

Until very recently, western theorists and policymakers on cyber issues were by contrast broadly unreceptive to the notion of harmful content. The notion of free expression of opinion or viewpoint constituting a danger was seen as something wild and exotic, and rejected *a priori*, while freedom of expression and free movement of information across borders was held as sacrosanct. This basic assumption has now changed beyond recognition, in the face of two distinct challenges to Western societies: Russian infowar activities centred around the conflict in Ukraine; and Islamic State (hereafter ISIS) with its own specific aims.

In Western exploration of these two problem sets, they are found to show similarities but also to be essentially distinct: in fact considerable debate has been devoted to which of the two is the more immediate threat to the West, Russia or ISIS[2]. In both cases, a key element of the challenge is «a multi-tiered online media operation in which a number of production units... produce content consistent with the core...

---

[1] As with Keir Giles, «Hall of Mirrors — Foreign Perception of Russian Information Security Concerns», Proceedings, Seventh International Forum «Partnership of State Authorities, Civil Society and the Business Community in Ensuring International Information Security», Garmisch-Partenkirchen, Germany, April 2013, pp. 238–245.

[2] «NATO and New Ways of Warfare: Defeating Hybrid Threats», NDC Conference Report, NATO Defense College No. 03/15, NATO Defense College, Rome, May 2015.

message»[3]. The result of both is that for the first time in generations the West has been forced to consider the application of the liberal principles of freedom of expression in a practical applied context — not on the basis of idealism, but dealing with a problem which is real and immediate.

Specifically in cyber terms, the Ukraine conflict in particular has the potential to bring about a transformative effect on cyber doctrine. Unlike Russia, the siloed Western approach to cyber has typically focused on technical responses to technical threats, largely disregarding the interface with information warfare in the broad sense. This approach is entirely apt for persistent or background threats, but probably insufficient for when a crisis emerges, since at that point there will be no such thing as "pure cyber" confrontation. In other words, the West may have been well prepared for cyber war, but events in Ukraine show that it also needs to be prepared for information war when cyber operations are used as a facilitator.

The exceptions to this rule were previously found in specialised areas of information warfare science: those strictly limited to military operations (although even here, the wide range of caveats and disclaimers applied by individual countries to NATO doctrine indicates the controversial nature of the issue)[4]; and, more recently, study of use of social media for influence purposes, up to and including regime change (although even during the Arab Spring, in the West this received attention only from a narrow circle of specialists).[5] But recent events have provoked a much broader shift in the conceptual framework of information threat by Western media, leadership and society in a substantially new information threat environment, embodying recognition that hostile information in the form of content, as well as code, brings with it problems and challenges. The irony is that this is in effect a move toward the Russian view of information security.

Vulnerabilities

Both Russian and ISIS information campaigns astutely target inherent weaknesses in Western liberal democratic societies, and exploit a range of self-inflicted vulnerabilities which are fundamental to those societies' views of themselves and their values.

---

[3] «Violent Islamist Extremism, The Internet, and the Homegrown Terrorist Threat», United States Senate Committee on Homeland Security and Governmental Affairs, 8 May 2008, http://www.hsgac.senate.gov//imo/media/doc/IslamistReport.pdf

[4] Referenced in NATO publication AJP-3.10, «Allied Joint Doctrine For Information Operations».

[5] As, for example, Scott Railton, «Revolutionary Risk-Cyber Technology and Threats in the 2011 Libyan Revolution», US Naval War College, 2013.

These include:

- Dogmatic dedication to freedom of expression as an absolute;
- Powerful liberal media, with their own sometimes peculiar notions of what serves national security interests;
- Within those media, a preference for balance over objectivity;
- The trend for user-generated content over the last 15 years, including now ubiquitous platforms for readers and listeners to add their own comments to media reportage;
- Political leaders receiving largely the same information flows as their electorate, and being sensitive to them in the same ways.

Each of these provides a distinctive vector for those who wish to manipulate information in order to achieve a social or political effect. And in each case, the role of social media acts as both an access channel and an operating environment. Both actors capitalise on the belated recognition that "digital media are becoming the main — and for a growing number of young people, the only — channel for political information and communication. They are the primary space for political activities, where citizens receive political information, shape their political views and beliefs, and have the opportunity to influence the processes related to functioning of power"[6] — and that consequently, «new social media have become the most effective tool for influencing the minds of huge communities, even whole nations»[7].

In the Russian case, cyber activities in the broad sense are critical to offensive disinformation campaigns, whether establishing sources for disinformation by setting up false media outlets online[8], or using social media to address targets of opportunity for subversion and destabilisation efforts apparently unrelated to events in Ukraine[9]. These activities are augmented by the ubiquitous activities of trolls and bots, which exploit specific features of the relationship between traditional and social media in order to both plant, disseminate and lend credibility to disinformation[10]. They combine for effect with a broad range of other measures such as Russian propaganda outlets being coy about

---

[6] Velichka Milina, «Security in a Communications Society: Opportunities and Challenges», Connections, Spring 2012, Volume XI, Number 2, p. 55.

[7] *Ibid.*

[8] Dalibor Rohac, «Cranks, Trolls, and Useful Idiots: Russia's information warriors set their sights on Central Europe», Foreign Policy, 12 March 2015, https://foreignpolicy.com/2015/03/12/cranks-trolls-and-useful-idiots-poland-czech-republic-slovakia-russia-ukraine/

[9] Doug Bernard, «America's Adversaries Use Baltimore Unrest to Spread Anti-US Message», VOA News, 30 April 2015, http://www.voanews.com/articleprintview/2743166.html

[10] Polina Tikhonova, «Russia Hacking Your News», ValueWalk, 14 March 2015, http://www.valuewalk.com/2015/03/russia-hacking-your-news/

their affiliation in order to seduce viewers in the United States and elsewhere[11], links with far-right political parties to garner direct political influence[12], and old-school subversive measures such as «NGO diplomacy, or establishing and assisting pro-Russian youth groups, minority and separatist organisations, and think tanks abroad»[13]. The result is that externally, the multiplicity of deceptive narratives put forward by Russian information campaigns finds fertile ground among populations which are not well informed on the realities of history, geography, and the issues at stake in Ukraine.

These populations, and in particular their free media, proved entirely unprepared in early 2014 for resisting a coordinated information warfare onslaught[14]. Western societies put faith in their own independent media to arrive at and report the truth thanks to their relative freedom of action. But Western liberal media training proved initially to be no match for the unity of message emanating from Russia. In fact, the opposite was true: the emphasis on balance in many Western media ensured that adversarial narratives, no matter how patently fraudulent, were repeated to European and American audiences by their own media. Whether the issue was ISIS overstating its power and reach, or the wide range of narratives supporting Russian public diplomacy, this balance imperative resulted in news editors rigidly following the dictum that there must be two sides to every story — even when in reality, there is only one[15]. Consequently, even when presented with known disinformation, Western news editors had little choice but to report it — hence lending that version weight and authority.

Here, too, the internet and social media played their own distinctive role. In the Russian case, the Kremlin troll army interacting directly with readerships in a range of fora including online discussion boards, Twitter and more, acted as a force multiplier for driving home

---

[11] Jill Dougherty, «Russian TV's American Face», Huffington Post, 4 November 2014.

[12] ««Черный интернационал». Как Москва кормит правые партии по всему миру», The Insider, 27 November 2014, http://theins.ru/politika/2113. See also Andrew Higgins, «Waving Cash, Putin Sows E.U. Divisions in an Effort to Break Sanctions», New York Times, 6 April 2015, http://nyti.ms/1ac5osT

[13] Sinikukka Saari, «Russia's public diplomacy: soft tools with a hard edge», Border Crossing (Diplomat Magazine), April 2015.

[14] Nick Cohen, «Russia Today: why western cynics lap up Putin's TV poison», The Observer, 8 November 2014, http://www.theguardian.com/commentisfree/2014/nov/08/russia-today-western-cynics-lap-up-putins-tv-poison

[15] As explored in a Norwegian context by Kjell Dragnes in «Journalister i propagandaens tid», Aftenposten, 23 March 2015, http://www.aftenposten.no/meninger/Journalister-i-propagandaens-tid-7954103.html

the Russian message — especially by diverting or suppressing any debate which pointed out the inconsistencies or implausibilities of the Russian version of events. The resulting scale, intensity, volume and consistency of the Russian arguments online, with a consistent version of events being repeated by all levels of the Russian media machine from the President to the lowliest foot soldier in the Kremlin troll army, continues to exacerbate the Western media problem of favouring balance over objectivity, and can result in reporting being further skewed by taking into account the entirely false, but ubiquitous, Russian alternate narrative.

Thus Western media in particular proved themselves entirely unprepared to resist a coordinated and well-resourced information campaign. This led at first to striking success in penetration of narratives, which contributed powerfully to Russia's ability to prosecute operations against Ukraine in the early stages of the conflict with little coordinated opposition from the West. The fact that for almost a year the EU found itself unable to refer publicly to the presence of Russian troops in Ukraine[16] denotes a broader inability to challenge the Russian version of events — without which a meaningful response is impossible. Early media coverage of the conflict made it «apparent, in short, that some interlocutors had swallowed whole some of the cruder falsifications of Russian propaganda»[17].

By comparison with the pre-internet era, the effective seeding of these falsifications is vastly simpler. Noisy and unsubtle exploits like hacking the Twitter feed of a major news agency to plant disinformation[18] have taken place, but even these are entirely unnecessary when stories can be introduced into media by other, seemingly natural and legitimate, means. Major commercial news media outlets in Western nations have made substantial cuts in reporting staff as advertising revenue has bled away to other media, and few of the numerous amateur blogs and forums which have sprung up have the capacity for serious source validation on their own. Consequently, sock puppet websites which appear to provide or aggregate news can achieve substantial reach and penetration. Once the disinformation placed there has been

---

[16] Andrew Rettman, «EU breaks taboo on 'Russian forces in Ukraine'», EU Observer, 16 February 2015, https://euobserver.com/foreign/127667

[17] John Besemeres, «Russian disinformation and Western misconceptions», Inside Story, 23 September 2014, http://insidestory.org.au/russian-disinformation-and-western-misconceptions

[18] «AP Twitter hack causes panic on Wall Street and sends Dow plunging», The Guardian, 23 April 2013, http://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall

fed into the mainstream news stream at one or more points, and is picked up and reported by reputable traditional media whose editors and reporters have not grasped that it is disinformation, others will follow: even in the new climate of awareness, major news media do not wish to be left behind on a story which has made it to the news agenda.

Denial

As the realisation of the nature of the Russian information campaign began to filter through Western media and policy-making circles, this gave way to a dangerous optimism about the effectiveness of Russian measures, and a widespread assumption that Russian disinformation was failing because of its lack of plausibility[19]. Supposedly, Russian fabrications and denials were ineffective because they were so obvious that they did not confuse senior, or intelligent, individuals in the West. This argument was seductive: by Western criteria, a significant proportion of Russian disinformation appears clumsy, counter-productive, obvious, and easily debunked. But assessing the campaigns by these standards carried a significant risk of misinterpreting Russian objectives. In particular it led initially to underestimating the effects of layered messaging, of more subtle campaigning screened and concealed by the obvious, of continued saturation, and the pernicious effect of the «filter bubble» on online reading habits. In particular, it failed to account for the initial lack of visibility on disinformation and hostile propaganda being disseminated not only in European languages, but also in Arabic — and Russian — targeting minorities in European nations.

Measured by Russian criteria instead, the information campaign has in fact made substantial achievements. This is particularly the case in two key areas: internally, controlling the domestic media environment; and externally influencing mass consciousness, and creating an environment where it is hard to distinguish quality information, in order to undermine the objectivity of Western media reporting and hence influence the information available to policymakers (a senior correspondent for a respected British national newspaper was still saying in April 2015 that the large numbers of e-mails and comments and responses through social media that were in support of Russian policy indicated a real groundswell of opinion among the readership). Together, these

[19] As for instance Professor Lawrence Freedman: «efforts at deception were by and large ineffectual, as the Russian role became progressively transparent.» Lawrence Freedman, «Ukraine and the Art of Limited War», Survival: Global Politics and Strategy, 56:6, 7-38 (2014).

form a combined defensive and offensive strategy working through both domestic and external media[20].

Responses — Government

in September 2011, an in-depth report issued by the UK think-tank Chatham House identified scope for substantial improvement in strategic communications policy and implementation by Western governments, even before these governments were subjected to the current stress test of sustained hostile information campaigning.[21] And at a governmental and supranational level, the eventual shape of overall responses to the new information warfare threat remains at the time of writing unclear. Discussion of information warfare as a problem has been subsumed into debate over the «new» form of warfare overall — whether described as ambiguous, non-linear, asymmetric or hybrid. But some clear themes have already emerged regarding the responses that Western governments are not considering. Four distinct tactics for defence against information warfare appear already to have been ruled out.

1. *There will be no restrictions on freedom of expression, and no direction of the media.*

This approach, on the rare occasions when the topic has even been raised, appears to have been rejected immediately and categorically. Content control, or censorship of opinion — whether that opinion is genuinely held or paid for — is not an option for Western liberal democracies. Leaderships in these societies continue to espouse liberal values, and reject any copying of Russian measures for control of domestic public opinion. They follow the principle established in 1946 by US diplomat George Kennan, that "the greatest danger that can befall us in coping with this problem... is that we shall allow ourselves to become like those with whom we are coping"[22].

2. *There will be no symmetric response to hybrid campaigns. In particular, Western governments will not engage in systematic disinformation campaigns*[23].

---

[20] Matthew Armstrong, «Russia's War on Information», War on the Rocks, December 2014, http://warontherocks.com/2014/12/russias-war-on-information/

[21] Paul Cornish, Julian Lindley-French and Claire Yorke, «Strategic Communications and National Strategy», Chatham House report, September 2011.

[22] Telegram, George Kennan to George Marshall, 22 February 1946, available at https://www.trumanlibrary.org/whistlestop/study_collections/coldwar/documents/pdf/6-6.pdf

[23] «Ümarlaud: Vene propaganda vastu võitlemise asemel tuleb pakkuda alternatiivi», Postimees, 18 February 2015, http://www.postimees.ee/3096321/umarlaud-vene-propaganda-vastu-voitlemise-asemel-tuleb-pakkuda-alternatiivi

Multiple conflicting untruths are a key element of the Russian approach to information warfare. But held to account by liberal media and critical societies, Western leaders know that any lies will be short-lived and counter-productive. Their only option in response is to stick rigidly to the truth.

3. *There will be no introduction of the concept of national information space, and consequently no notion of "breaches" in that space, as described in Russian information security doctrine.*

It is still taken for granted that the internet by its very nature depends on the free and unimpeded passage of information across national boundaries, and there has been no suggestion of preventing it from doing so.

4. *There are no visible moves as yet toward setting up national bodies within government tasked with defensive strategic communications — in other words, countering information warfare.*

Some limited moves toward an integrated approach to information warfare are visible in a military context, for example with the establishment of the UK's 77 Brigade, bringing together a number of different units active in different domains of Information Activities (IA). But the overall tasks of tracking and countering disinformation remain primarily delegated to voluntary or non-governmental organisations like Bellingcat[24], The Interpreter[25] or Stopfake[26], with no evident government or international involvement.

Responses — Public

Elsewhere, the diffused, uncoordinated and self-regulating nature of social media has facilitated effective self-defence mechanisms. A new alertness to the prevalence of orchestrated troll campaigns has led to the dissemination of self-help guides for dealing with trolls in the absence of moderation[27], and the growing availability of tools for detection of troll and bot campaigns is assisting in spreading awareness[28]. As a result, according to one Russian assessment, despite the «billions of dollars» spent by the Russian state on attempting to «turn social networks into its obedient weapon», «net society has developed immunity.

---

[24] https://www.bellingcat.com/tag/russia/

[25] http://www.interpretermag.com/about-us/

[26] http://www.stopfake.org/en/news/

[27] A popular infographic depicting «The Five Stages of Arguing with a Russian Nationalist» is a prime example, available at http://i.imgur.com/ka4Gmd0.jpg

[28] Lawrence Alexander, «A Response to the KremlinBot Skeptics», Global Voices, 24 April 2015, http://globalvoicesonline.org/2015/04/24/a-response-to-the-kremlin-bot-skeptics/print/

Now the negative effect from the Kremlin's efforts to manipulate the opinion of net society is such that it de facto negates these efforts»[29].

Awareness of the destructive potential of hostile information campaigns is also growing in fields which are entirely unrelated to state or non-state adversaries such as Russia or ISIS. The phenomenon of source proliferation sowing doubt in authoritative sources has been noted in science, with the problem of "predatory journals" diluting properly peer-reviewed scientific journal articles with unevaluated material, leading to readers being "unable to distinguish between credible research and junk science"[30]. And in the UK, controversy over local elections in the London district of Tower Hamlets brought widespread attention to the vulnerabilities of liberal political processes to subversive information campaigns. This incident demonstrated how a dedicated group of individuals can seize political power using concerted efforts to target a specific community's points of susceptibility, by means of intimidation, disinformation, making use of cultural and religious sensitivities, and targeting the disaffected — tapping into existing or manufactured senses of grievance or exclusion[31].

By the end of 2014, Western media outlets were still faithfully reporting Russian disinformation as fact, but the realisation that they had been subjected to a concerted campaign of subversion was beginning to filter through into reporting. In traditional media (including their online versions), this was evidenced in the closure or moderation of previously open-access discussion boards, and the rolling back of user-generated content. References to social media were also been curtailed in the face of concerted troll offensives. Paradoxically, one of the first major news outlets to take these steps was *The Guardian* in the UK — previously a bastion of liberal extremism and freedom of expression, to the extent that at the height of the Snowden controversy, its editors viewed themselves as the self-appointed arbiters of whether the publication of stolen classified information was in the national interest[32].

---

[29] «Владимир Голышев: "В информационной войне надо «идти на грозу»"», Russkiy Monitor, 29 January 2015, http://rusmonitor.com/vladimir-golyshev-v-informacionnojj-vojjne-nado-idti-na-grozu.html

[30] Robert E Bartholomew, «Science for sale: the rise of predatory journals», Journal of the Royal Society of Medicine: 2014, Vol. 107(10), pp. 384–5.

[31] "Judgment In The High Court Of Justice, Queen's Bench Division, In The Matter Of The Representation Of The People Act 1983 And In The Matter Of A Mayoral Election For The London Borough Of Tower Hamlets Held On 22 May 2014", available at http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/judgment.pdf

[32] Keir Giles, «Legitimation of Online Surveillance and Monitoring», conference paper, Eighth International Forum «Partnership of State Authorities, Civil Society and the Business Community in Ensuring International Information Security», April 2014.

But recognition by individual media that their objectivity and independence are being subverted by Russian disinformation and troll campaigns[33] have not generally translated into a coordinated response. In particular, the imperative of «balance» still presents a key challenge. As a result of the balance requirement, even a report by a respected diplomatic correspondent explaining the nature of «hybrid warfare» — the term broadly adopted by the West to describe the nature of the Russian campaigns in and around Ukraine — needs to include six paragraphs of Russian denial, claiming the whole concept is a Western fabrication intended to discredit Russia[34].

National external broadcasters in the West have been presented with a different problem. Deutsche Welle, the BBC World Service, Radio Free Europe and others have been tasked with reaching Russian audiences in order to counter the alternative reality established in the Russian media space, with particular reference to Russian combat operations in Ukraine. For Western military forces, media consciousness is an integral part of operational planning. This is due to the recognition that the proliferation of mass media and instant communications has made it «possible for the citizens of a nation to scrutinise the conduct of war by their military forces... [leading to] the possibility of a public opinion directly impacting the political decision-making of a nation»[35]. But in 2015 this is an asymmetric vulnerability, since it applies to Western liberal democracies with a free media, but not — as conclusively demonstrated by events around Ukraine — to Russia.

Instead, Russia has undertaken a range of effective measures to insulate itself from this scrutiny by its own population. These measures include ways of isolating Russians from external sources of information — putting in place both overt and covert elements of what Daniel Schearf, Moscow Bureau Chief for Voice Of America, describes as a new "media Iron Curtain"[36]. This leaves domestic information space entirely dominated by state media, with central direction of the Russian domestic news agenda long pre-dating operations in Ukraine[37]. The result is an

---

[33] Chris Elliot, «The readers' editor on... pro-Russia trolling below the line on Ukraine stories», The Guardian (May 4, 2014), http://www. theguardian.com/commentisfree/2014/may/04/pro-russia-trolls-ukraine-guardian-online

[34] Bridget Kendall, «Hybrid warfare: The new conflict between East and West», BBC News, 6 November 2014, http://www.bbc.co.uk/news/world-europe-29903395

[35] Sanu Kainikara, «Air Power in the Information Age: The Deciding Factor», Air Power Development Centre [Australia], February 2015, p. 3.

[36] Conversation with author, August 2015.

[37] Stephen Castle, «A Russian TV Insider Describes a Modern Propaganda Machine», New York Times, 13 February 2015, http://nyti.ms/1zcDqDq

unrecognisable Russian alternative reality[38], where «the Russian media, with very few exceptions, have abandoned, sometimes through coercion, but mostly voluntarily and even eagerly, their mission of informing the public and have turned into creators of the Matrix-like artificial reality where imaginary heroes and villains battle tooth and nail in Russia's Armageddon»[39]. What remains of Russia's free media have largely been either marginalised, or intimidated into compliance[40]. Consequently, foreign state broadcasters are under considerable pressure by their funding governments to «do something» in order to fulfil their mission of communicating external reality to the Russian media audience.

In doing so they face new challenges. During the Cold War, when these broadcasters were last faced with a similar requirement, the primary method of delivery was short wave radio. But today, even if potential listeners still possessed short wave receivers, the cost and complication of regenerating this kind of broadcast capability would render it unfeasible. Meanwhile, the rebroadcasting licences which were issued in Russia during an earlier period of free media cooperation, allowing foreign broadcasts on FM in major cities, have been revoked or not renewed. In 2015, the notion of foreign broadcasters being allowed the kind of access to the Russian media market that RT enjoys in the West seems impossibly remote[41]: in particular because in Russian doctrine, any such access which provides an alternative to the official state version of events is interpreted as being immediately and directly hostile[42].

Outlook

Throughout 2015, initial concern in the West over information campaigns facilitating future Russian assertive action in eastern Eu-

---

[38] Gary Shteyngart, «Out of My Mouth Comes Unimpeachable Manly Truth», New York Times, 18 February 2015, http://www.nytimes.com/2015/02/22/magazine/out-of-my-mouth-comes-unimpeachable-manly-truth.html?emc=eta1&_r=0

[39] Vasily Gatov, «How the Kremlin and the Media Ended Up in Bed Together», The Moscow Times, 11 March 2015, http://www.themoscowtimes.com/opinion/article/how-the-kremlin-and-the-media-ended-up-in-bed-together/517323.html

[40] Andrei Malgin, «Russia's State Media Get Away With Murder,» The Moscow Times, 4 November 2014, http://www.themoscowtimes.com/opinion/article/russia-s-state-media-get-away-with-murder/510619.html. See also «Russian media firms: Interesting news», The Economist, 8 November 2014, http://www.economist.com/node/21631057/print

[41] Keir Giles, «The information war: how Moscow controls access to Western media», The World Today, August-September 2015, p. 19.

[42] Vyacheslav Nechayev, «США вводят информационные войска в российские социальные сети», Izvestiya, 14 April 2015, http://izvestia.ru/news/585366

rope has been augmented by alarm at the potential consequences of the information isolation of Russia itself. For the majority of the Russian population, even those that take an informed interest in outside events, access to external reality is becoming more challenging. Portals such as *InoSMI* provide the semblance of a window onto the outside world, but in fact selectively translate and distort media reports in order to support the official Russian state version of events, augmenting a view of the world which is unrecognisable from the original[43].

The existence of this fundamental disparity between perception within Russia and reality outside it poses a number of significant dangers. These include, but are not limited to, reinforcing the perception that the independent nations of the former Soviet Union, including Ukraine and the Baltic States, in effect belong to Russia: as expressed by President Putin's comment that in 1991 «Russia voluntarily — I emphasise — voluntarily and consciously made absolutely historic concessions in giving up its own territory»[44].

In some sectors of Russian society, these aspirations by Russia to regain imperial dominion over its surroundings have always enjoyed broad support — the now-celebrated Prosecutor General of Crimea, Natalya Poklonskaya, in an interview at the time of annexation declared her ambition to "start again in a great state, a great power, an *empire*, like Russia"[45]. But the current information campaigns provide a permissive environment for the rise of the rhetoric of confrontation, which carries dangers of its own. Intensive militarisation — sometimes referred to directly as mobilisation — appears from the outside to be pervading Russian society, stoked by unending leadership rhetoric of war, confrontation and threat, and blanket military coverage on TV. The state-led narrative of war is "instrumentalising the population and putting it on a mental war footing", not only by tapping into the traditional Russian narrative of victimhood over centuries, but also by engendering "a heroic feeling that now is the time of risk"[46]. To the bemusement of the West, Russian leadership figures state that «Americans are trying to involve the Russian Federation in interstate military

[43] Rolf Fredheim, «Filtering Foreign Media Content» How Russian News Agencies Repurpose Western News Reporting», Journal of Soviet and Post-Soviet Politics and Society, Vol. 1, No. 1 (2015), pp. 37–83.

[44] Ksenia Kirillova, «Путин фактически назвал Украину территорией России», Novyy Region 2, 28 April 2015, http://nr2.com.ua/blogs/Ksenija_Kirillova/Putin-fakticheski-nazval-Ukrainu-territoriey-Rossii-95566.html

[45] Russian television interview available at https://www.youtube.com/watch?v=XX4JCQViRKg (at 2'40").

[46] Estonian Ambassador to the Russian Federation Jüri Luik, speaking at the Lennart Meri Conference, Tallinn 24 April 2015

conflict, to facilitate the change of power by way of using the events in Ukraine, and ultimately to carve up our country»[47].

Most dangerously, analysis of Russian security thinking shows not only this asymmetry of threat perception, but also a complete divergence with the West in terms of notions of how and when military force should be used to counter those threats. The new emphasis on the potential for use of nuclear weapons in statements by President Putin and other officials provides a particularly dangerous example[48]. In addition to the distinctive role which nuclear weapons play in Russian national identity[49], use of both strategic and tactical nuclear weapons now appears to be presented for Russian domestic consumption as «a realistic possibility»[50]. This gives rise to a dangerous mismatch of the unthinkable[51] — in the West, which has moved on from Cold War concepts of nuclear threat between major powers, these messages are received but not understood. Western media, societies and governments could have no better motivation for intensive effort toward understanding, and adapting for, the new environment of information confrontation.

---

[47] Interview with Security Council Secretary Nikolay Patrushev, *Rossiyskaya gazeta*, 11 February 2015.

[48] Tom Nichols, «If Putin goes nuclear», The War Room, 1 September 2014, http://tomnichols.net/blog/2014/09/01/if-putin-goes-nuclear/

[49] Tom Parfitt, «Ukraine Crisis: Putin's Nuclear Threats are a Struggle for Pride and Status», Daily Telegraph, 29 August 2014, http://www.telegraph.co.uk/news/worldnews/europe/russia/11064978/Ukraine-crisis-Putins-nuclear-threats-are-a- struggle-for-pride-and-status.html. For a more detailed examination of this phenomenon, see also Keir Giles and Andrew Monaghan, «European Missile Defense and Russia», U.S. Army War College Strategic Studies Institute, July 2014, http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1219.

[50] Stephen Ennis, «Russian media learn to love the bomb», BBC News, 23 February 2015, http://www.bbc.co.uk/news/world-europe-31557254.

[51] Alexander Golts, «Russia's Nuclear Euphoria Ignores Reality», Moscow Times, 6 October 2014, http://www.themoscowtimes.com/advertorials/ opinion/Russia-s-Nuclear-Euphoria-Ignores-Reality/

В.И.Гасумянов
ОАО «ГМК «Норильский никель»

Подходы ОАО «ГМК «Норильский никель» к проблемам формирования системы международной информационной безопасности

Разрешите от имени российской горно-металлургической компании «Норильский никель» поприветствовать организаторов и участников Девятого международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности». «Норильский никель» является крупнейшей компанией в мире по производству никеля и палладия, четвертой в мире по производству платины и одной из ведущих по производству меди, кобальта и родия. На сегодняшний день Норильский никель располагает производственными активами в четырех странах мира — России, ЮАР, Финляндии и Австралии. В 2013 году на предприятиях Компании было выпущено 285 тыс. тонн никеля, 371 тыс. тонн меди, 2 662 тыс. унций палладия и 651 тыс. унций платины. На сегодняшний день 4,3 % российского экспорта приходится на предприятия ГМК.

«Норильский никель», являясь системообразующей компанией, вносит значительный вклад в социально-экономическое развитие регионов России, поскольку Норникель зарегистрирован на территории РФ и все налоги уплачиваются в России. Большинство предприятий, входящих в Группу, имеют статус градообразующих.

В 2014 году «Норильский никель» представил обновленную стратегию развития ГМК. Новые стратегические подходы к управлению бизнесом с акцентом на возврат на вложенный капитал позволили Норникелю создать дополнительную экономическую стоимость. Подтверждением позитивной динамики стал пятикратный рост свободного денежного потока, несмотря на неблагоприятную рыночную конъюнктуру. По определению генерального директора компании В.О. Потанина, суть новой стратегии в том, что Норильский никель «сосредоточился на российских первоклассных активах, и вкладывает средства в их развитие на Кольском полуострове, в Норильском промышленном районе и в Забайкальском крае».

Принятие новой стратегии заставило ГМК пересмотреть подходы к обеспечению безопасности. Этот шаг также был продиктован изменившейся внешней средой, отличительной особенностью которой является формирование широкого спектра диверсифицированных рисков и угроз, как политического, так и экономического характера. С целью поступательной реализации системных решений в области безопасности, отвечающих перспективным интересам и планам Компании в рамках новой стратегии, Правлением ОАО «ГМК «Норильский никель» была принята концепция комплексной системы безопасности. В концепции содержатся принципиально новые предложения по совершенствованию архитектуры системы безопасности, основанные на апробированных современных российских и зарубежных подходах с использованием новейших методик и технологий.

Руководствуясь положениями утвержденной концепции, Норильский никель осуществил переход к новому принципу построения системы комплексной безопасности и ее управления. Был разработан и принят ряд целевых программ по обеспечению экономической, корпоративной, информационной, объектовой и транспортной безопасности. В результате создана современная мобильная система, позволяющая эффективно минимизировать производственные и финансовые риски, пресекать попытки хищений, проводить мероприятия по профилактике внутренней коррупции, по борьбе с незаконным оборотом драгоценных металлов и металлосодержащих материалов.

Для научно-методологического обеспечения этой деятельности в 2014 году учреждено дочернее предприятие «Институт современных проблем безопасности», занимающееся разработкой новых методов защиты законных интересов Компании, изучением и внедрением зарубежного опыта, проведением экспертных оценок, подготовкой аналитических документов.

ГМК «Норильский никель» ведет активную международную деятельность, направленную на повышение уровня безопасности в сфере производства и торговых операций с драгоценными металлами. Представитель Компании возглавляет комитет безопасности Международной ассоциации производителей металлов платиновой группы, в рамках которой, совместно с межрегиональным научно-исследовательским институтом Организации объединенных наций по вопросам преступности и правосудия (UNICRI) и правоохранительными органами ЮАР, активно участвует в программах по противодействию незаконному обороту

сырья драгоценных металлов и по борьбе с транснациональной преступностью.

Из вышесказанного можно сделать вывод о том, что «Норильский никель», как глобальная компания, оперирующая в динамично меняющемся политическом и бизнес- климате, реализующая многоплановые и многосторонние контакты на деловом и межгосударственном уровнях с зарубежными партнёрами в глобальных информационных сетях, неизбежно является объектом реальных и потенциальных угроз в сфере международной информационной безопасности. Причем, как мы знаем, в современном мире угрозы эти растут в геометрической прогрессии. Появление их все чаще имеет не криминальную, а политическую и идеологическую основу. Целью таких угроз становится нанесение вреда государствообразующим инфраструктурам и распространение экстремистской идеологии.

Ярким примером подобной деятельности является активность террористической организации «Исламское государство» (ИГ), запрещенной на территории России. В прошлом году ИГ начала действовать в киберпространстве, ее члены объединились в подразделение Cyber Caliphate, взломавшей Twitter-аккаунты Центрального командования США и журнала Newsweek. Там хакеры оставили угрожающее приветствие семье американского президента. Мишенью ИГ стали и российские Интернет-ресурсы. С 2014 года было атаковано 586 российских сайтов, принадлежащих государственным, научным и бизнес-структурам. Особенность этих атак является то, что в действиях хакеров ИГ отсутствует логика. Объектом следующей атаки может стать любой Интернет-ресурс. Хакерские группировки ИГ ведут аккаунты в социальных сетях Twitter, Facebook, Youtube и Google+, в которых рассказывают об успешных атаках. Кроме того, ИГ использует российские и иностранные социальные сети для вербовки новых членов организации. По информации, распространенной ФСБ, среди членов ИГ уже порядка двух тысяч россиян.

Что делать с подобными угрозами? Государство требует от Интернет-компаний блокировать активность кибертеррористов. Бизнес пытается самостоятельно бороться со злоумышленниками. Но отсутствие эффективного взаимодействия не останавливает исламистов, они уже создали собственную социальную сеть.

ГМК «Норильский никель» не является профильной компанией в области информационно-коммуникационных технологий, но проблемы международной информационной безопасности актуальны для нас и вызывают ряд опасений, которыми я хотел бы с

поделиться с экспертным сообществом. Для обеспечения непрерывности бизнеса, полного цикла производства, логистики и сбыта компания активно внедряет самые передовые информационно-коммуникационные технологии (ИКТ), инкорпорированные в глобальные информационные сети. В области обеспечения безопасности Норильский никель последовательно реализует шаги, направленные на создание новых международных инструментов с использованием информационно-коммуникационных технологий, в частности, в рамках Международной платиновой ассоциации. Но сегодня мы оказываемся в ситуации, когда политические риски безопасной, стабильной и отказоустойчивой работы Интернета в области международных коммуникаций многократно возросли. Односторонние санкции могут приводить к отказу от договорных обязательств, таких как сервисное обслуживание, техническая поддержка, обновление и др., со стороны мировых лидеров в области информационных технологий, находящихся вне юрисдикции России.

Следует учитывать, что предприятия Норильского никеля, являясь объектами критической инфраструктуры с точки зрения национальной безопасности, могут стать мишенью кибератак, инспирированных недружественными намерениями других государств. К сожалению, сейчас такая ситуация более чем реальна. В результате внешнеполитической активности некоторых стран в адрес России постоянно раздаются угрозы отключить или нарушить работу коммуникационных систем, обеспечивающих финансовую и экономическую деятельность страны и бизнеса, например, таких как SWIFT или электронных цепей стратегических поставок, что может нанести урон непрерывности бизнеса Норникеля. Возникает вопрос: какие причины лежат в основе этих угроз — только политические, или также экономические? Не используется ли осложнение международной ситуации недобросовестными конкурентами для реализации своих планов? Чтобы точно знать ответ, необходимо обеспечить транспарентность информации по всей линейке производитель-поставщик-потребитель. Потребитель должен иметь свои права, свой голос и присутствовать, и не только присутствовать, а активно участвовать в многостороннем диалоге по безопасности в киберпространстве. Иначе мы оказываемся заложниками межгосударственных отношений, производителей и поставщиков, что повышает риски, о которых я говорил выше — риски безопасной, стабильной и отказоустойчивой работы информационно-коммуникационных систем. В современном мире, про который можно смело сказать,

что он характеризуется хаосом в киберпространстве, активно идет дискуссия о необходимости выработки правил для трех акторов: государства, производителей и поставщиков информационно — коммуникационных технологий. Но нам представляется, что интересы тех, кто потребляет эту продукцию, использует ИКТ на стратегическом уровне в деловой активности и для обеспечения бизнес-процессов, не учитываются в достаточной мере. Главный вопрос — какие гарантии у потребителя, в данном случае у Норильского никеля, что мы сможем минимизировать риски столкновения с недружественными действиями в киберпространстве, инспирированными политическими или экономическими причинами. Именно с этим вопросом я хотел бы обратиться к экспертному сообществу, предложить проанализировать и сформулировать проблему с профессиональной точки зрения, а затем начать поиск приемлемых вариантов решения.

Вероятно, нужно начать многосторонний диалог и запустить процесс по выработке договоренностей и правил безопасности при производстве и поставках информационно-коммуникационных технологий. Это может стать одним из основных направлениями партнерства государства, бизнеса и общества при обеспечении международной информационной безопасности. Совместная работа по выработке и принятию указанных мер может обеспечить стабильность, безопасность и непрерывность функционирования сети Интернет. И если мы договоримся о принятии мер, то эти меры должны быть обязательными для исполнения, как на государственном уровне, так и для деловых кругов без исключения и оговорок.

Для реализации практических шагов сотрудничества, мы предлагаем создать в рамках Международного исследовательского консорциума информационной безопасности отдельное направление работы по указанной теме с участием представителей крупного российского и зарубежного бизнеса. Полагаю целесообразным подготовить предложения и вынести вопрос о разработке мер и правил с учетом интересов потребителей ИКТ для дальнейшего обсуждения в ходе очередной конференции Консорциума в Сеуле, осенью 2015 г. Начав эту работу и сформировав повестку, мы сможем затем реализовать ее, выйдя на уровень влиятельных мировых деловых форумов, расширяя сотрудничество бизнеса, экспертного сообщества в сфере обеспечения международной информационной безопасности с глобальными и региональными организациями, такими как ООН, ЕС, ОБСЕ, АСЕАН, ШОС, БРИКС. Надеюсь, что коллеги — представители государственных

и бизнес-структур, экспертного сообщества, поддержат Норильский никель в этом начинании.

В завершение своего выступления, я хотел бы подчеркнуть, что ГМК «Норильский никель» высоко оценивает работу по проблематике международной информационной безопасности, как в рамках текущей конференции, так и на площадках Международного исследовательского консорциума информационной безопасности. Мы считаем необходимым присоединиться к этой деятельности и внести свой вклад в качестве одного из крупнейших потребителей ИКТ и передовой компании мирового уровня.

Я хотел бы выразить искреннюю благодарность организаторам научного форума в г. Гармиш-Партенкирхен, сопредседателю оргкомитета конференции, директору Института проблем информационной безопасности МГУ В.П. Шерстюку, за приглашение и возможность поделиться с вами нашими подходами и предложениями. Учитывая чрезвычайную важность для бизнеса обсуждаемых здесь проблем, хотел бы выразить уверенность в нашем дальнейшем плодотворном сотрудничестве.

V.I.Gasumyanov
Norilsk Nickel (the Russian Federation)

Approaches of Norilsk Nickel to the issues of International Information Security System Development

On behalf of the Russian Mining and Metallurgical Company (MMC) Norilsk Nickel allow me to greet the organizers and participants of the Ninth International Forum «Partnership of State Authorities, Civil Society and the Business Community in Ensuring International Information Security». Norilsk Nickel is the largest company in the world in production of nickel and palladium, the fourth in the world in production of platinum and one of the leading companies in production of copper, cobalt and rhodium. Today Norilsk Nickel has production assets in four countries — Russia, South Africa, Finland and Australia. In 2013 the company produced 285 thous. tonnes of nickel, 371 thous. tonnes of copper, 2662 thous. ounces of palladium and 651 thous. ounces of platinum. To date, MMC's production amounts to 4.3% of Russia's exports.

Being a strategic company, Norilsk Nickel makes a significant contribution to the socio-economic development of the Russian regions, as Norilsk Nickel is registered in the Russian Federation and all taxes are paid in Russia. Most businesses in the Group have a city-forming status.

In 2014 Norilsk Nickel presented an updated strategy for MMC development. New strategic approaches to business management with an emphasis on return on invested capital have allowed Norilsk Nickel to create additional economic value. A confirmation of positive dynamics is a fivefold increase in free cash flow, despite unfavorable market conditions. By definition of director general V.Potanin, the essence of the new strategy is that Norilsk Nickel «has focused on the first-rate Russian assets and invests in their development on the Kola Peninsula, in the Norilsk industrial district and the Trans-Baikal region».

The adoption of the new strategy forced MMC to reconsider its approaches to security. This step was also dictated by the changed external environment, the distinguishing feature of which is the formation of a wide range of diversified risks and threats, of both political and economic nature. With a view to progressive implementation of comprehensive security solutions that meet the long-term interests and plans of the Company under the new strategy, the Board of OJSC

MMC Norilsk Nickel has adopted the concept of an integrated security system. The concept introduces fundamentally new proposals to improve the security architecture based on proven modern Russian and foreign approaches that utilize the latest techniques and technologies.

Guided by the provisions of the approved concept, Norilsk Nickel has made the transition to the new principle of construction and management of an integrated security system. There have been developed and adopted a number of targeted programs to ensure economic, corporate, information, facility and transport security. As a result, the company created an innovative mobile system that allows to effectively minimize operational and financial risks, to prevent attempts of theft, carry out activities to prevent internal corruption, to combat illicit trafficking of precious metals and metal-bearing materials.

For scientific and methodological support of this activity, a subsidiary «Institute of contemporary security challenges» has been established in 2014. It engages in the development of new methods to protect the legitimate interests of the Company, the study and implementation of international best practices, peer reviews, preparation of analytical documents.

MMC Norilsk Nickel engages in robust international activities aimed at improving of safety in production and trading of precious metals. The representative of the Company heads the security committee of the International Association of Manufacturers of platinum group metals, within the framework of which, together with the Inter-Regional Research Institute, the United Nations Interregional Crime and Justice Research Institute (UNICRI) and the law enforcement agencies of South Africa, he is actively involved in programs to combat illicit trafficking of raw material of precious metals and to combat transnational crime.

From the above it can be concluded that Norilsk Nickel, as a global company operating in a rapidly changing political and business climate, implementing multifaceted and multilateral contacts on business and interstate levels with foreign partners in the global information networks, is inevitably becoming an object of real and potential threats in the sphere of international information security. And as we know, in the modern world these threats are growing exponentially. Their manifestations increasingly have not criminal, but political and ideological basis. The aim of such threats is degradation of state-forming infrastructure and dissemination of extremist ideology.

A striking example of this is the activity of a terrorist organization «Islamic State of Iraq and Syria» (ISIS), banned in Russia. Last year ISIS began its operations in cyberspace; its members joined a Cy-

ber Caliphate division and hacked a Twitter account of the US Central Command and the Newsweek magazine. The hackers left there a threatening greeting to the family of an American president. Russian Internet resources have also become targets of ISIS. Since 2014 586 Russian websites of state, scientific and business structures have been attacked. The peculiarity of these attacks is that the actions of ISIS hackers have no logic. The object of the next attack could be any online resource. ISIS hacker groups have accounts in social networks, Twitter, Facebook, YouTube and Google+, where they tell about successful attacks. ISIS also uses Russian and foreign social networks to recruit new members. According to information released by the Federal Security Service of Russia, there are about two thousand Russians among the members of ISIS.

What can be done with these threats? The government requires Internet companies to block the activity of cyberterrorists. Business attempts to fight the attackers on its own. But due to the lack of effective interaction this cannot stop the Islamists, who have already set up their own social network.

MMC Norilsk Nickel is not a core company in the field of information and communication technologies, but the issues of international information security are relevant for us and raise a number of concerns that I would like to share with the expert community. To ensure business continuity, the full cycle of production, logistics and marketing the company is actively implementing the most advanced information and communication technologies (ICT) incorporated into the global information network. Considering security, Norilsk Nickel is consistently taking steps aimed at establishing of new international instruments using information and communication technologies, in particular, in the framework of the International Platinum Group Metals Association. But today we find ourselves in a situation when political risks of secure, stable and resilient operation of the Internet in the field of international communications have increased manifold. Unilateral sanctions could lead to repudiation of contractual obligations (such as after-sales service, technical support, updating, etc.) by the world ICT-leaders that are out of Russian jurisdiction.

It should be taken into consideration that Norilsk Nickel is a critical infrastructure from the point of view of national security, and thus may become a target of cyberattacks, inspired by unfriendly intentions of other nation-states. Unfortunately, today this situation is more than real. As a result of the activity of certain foreign countries, Russia is constantly threatened with shutdown or disruption of communication systems that support financial and economic activity of the country and

business, such as SWIFT or electronic strategic supply chains — that can damage Norilsk Nickel business continuity. The question arises: what causes underlie those threats — only political or economic as well? Is aggravation of international situation used by unfair competition for the realization of their plans? To accurately know the answer, it is necessary to ensure the transparency of data along the entire line of a manufacturer-supplier-consumer. Consumers should have their rights, their voice and be present, and not only be present, but actively participate in multilateral dialogue on cyberspace security. Otherwise we will find ourselves hostages to bilateral relations, manufacturers and suppliers, and this increases the risks that I mentioned earlier — the risks to secure, stable and resilient operation of information and communication systems. In the modern world, which we can safely say to be characterized by chaos in cyberspace, there is an active discussion underway about the need to develop rules for three actors: the state, manufacturers and suppliers of ICTs. But we believe that the interests of those who use these products and ICTs at the strategic level of business activity and to support business processes are not adequately considered. The main question — what guarantees does the consumer, in this case, Norilsk Nickel have, that we can minimize the risks of facing unfriendly actions in cyberspace, inspired by political or economic reasons. It is the question with which I would like appeal to the expert community, to offer to analyze and formulate the problem from a professional point of view, and then start the search for acceptable solutions.

Perhaps it is necessary to start a multilateral dialogue and begin development of agreements and rules of safety for manufacturing and supply of ICTs. This may be one of the main directions of partnership between nation-states, business and society in ensuring international information security. Joint efforts on development and adoption of these measures can ensure stability, security and continuity of the Internet. And if we agree to adopt the measures, these measures must be binding for both the nation-states and for the business community, without exceptions or reservations.

To implement the practical steps of cooperation, we propose to open a separate relevant venue of research at the International Information Security Research Consortium with the participation of representatives of major Russian and foreign businesses. I deem it appropriate to prepare proposals on the development of policies and regulations with respect to the interests of ICTs consumers and submit them for further consideration at the next Consortium meeting in Seoul in autumn 2015. Once we begin this work and form the agenda, then we will

be able to implement it, coming to the level of influential international business forums, expanding cooperation of businesses and experts in the field of international information security with global and regional organizations, such as the UN, the EU, the OSCE, the SCO, ASEAN and BRICS. I hope that the colleagues — the representatives of governmental and business structures and of expert community will support Norilsk Nickel in this endeavor.

In conclusion to my presentation, I would like to emphasize that MMC Norilsk Nickel appreciates the work on the issues of international information security within the ongoing conference, and at the venues of International Information Security Research Consortium. We consider it necessary to join this activity and to contribute being one of the largest ICT consumers and a progressive world-class company.

I would like to express my sincere gratitude to the organizers of the scientific forum in Garmisch-Partenkirchen, to the co-chairman of the Organizing Committee, Director of the Institute of Information Security Issues at MSU V.P.Sherstyuk for the invitation and the opportunity to share with you our approaches and proposals. Since the issues discussed here are of critical importance to business, I would like to express confidence in our further fruitful cooperation.

С.В.Устюгов

Корпорация ZTE (Китай)

Основные приоритеты корпорации ZTE по вхождению на российский рынок и укреплению международной информационной безопасности

В своем выступлении мне хотелось бы отметить важность Форума с точки зрения корпорации ZTE, сказать несколько слов о сегодняшнем положении корпорации ZTE на мировом рынке телекоммуникаций, а также основных принципах и направлениях ее работы в России.

Прежде всего, позвольте передать приветствия организаторам и участникам форума от имени Президента ZTE corporation господина Ши Лижуна (Shi Lirong), от руководства российской дирекции ZTE corporation, от себя лично и пожелать всем присутствующим успехов, здоровья и благополучия. Выражаем также благодарность за приглашение принять участие в работе Девятого международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности».

За прошедшие годы Форум превратился в важный инструмент консолидации усилий IT-специалистов многих стран в противодействии угрозам кибертерроризма и кибервойн. Благодаря Форуму, в работе которого принимают участие ведущие специалисты и ученые заинтересованных стран, фактически сформирована новая общечеловеческая ценность — система международной информационной безопасности. Её главную ценность определяет совокупность правил использования информационно-коммуникационных сетей и система критериев оценки действий субъектов глобальной коммуникации.

Такая оценка значимости Форума позволяет провести ряд аналогий. Например, ни у кого не вызывает сомнений важность для любого сообщества наличия конституции — основного закона, по которому оно живет. Именно он позволяет сообществу квалифицировать хорошее и плохое, принять нормы права, которые определяют ответственность граждан за свои действия. Однако в глобальном киберпространстве таких правил пока нет.

В связи с этим можно утверждать, что совместными усилиями специалистов многих стран в рамках Форума формируется не-

кий прообраз Всеобщего Закона сети Интернет, который помимо определения правил поведения и ответственности субъектов глобальных коммуникаций, мог бы содействовать укреплению сотрудничества различных стран на основе формирования доверенной информационной среды.

Это особенно актуально в условиях, когда информационная сфера используется отдельными государствами для ужесточения диктата в отношении как своих партнеров и союзников, так и стран, желающих проводить самостоятельную политику. Поэтому сегодня как политические, так и технологические решения по обеспечению международной информационной безопасности остро востребованы многими представителями международного сообщества. Известно, что сложные условия бывает легче переносить на основе объединения усилий партнеров.

В таких условиях отношения между Российской Федерацией и Китайской Народной республикой стали обретать черты стратегического партнерства. К числу компаний, которые стремятся внести свой вклад в укрепление российско-китайского сотрудничества, посредством расширения взаимодействия с российскими потребителями высокотехнологической продукции, относится и корпорация ZTE.

Присутствие на российском рынке и стратегия корпорации ZTE в России не очень широко освещается в СМИ. Поэтому хотелось бы сказать несколько слов о корпорации ZTE. Корпорация ZTE образована в 1985 году. По форме организации ZTE является открытым акционерным обществом с контрольным пакетом акций китайской аэрокосмической корпорации. Указанная корпорация является государственной. По направленности деятельности ZTE является одним из крупнейших производителей связного и телекоммуникационного оборудования не только в КНР, но и во всем мире. Филиалы корпорации присутствуют в более чем 100 странах. В КНР и за рубежом эффективно функционируют 18 научно-исследовательских центров. Деятельность Корпорация ZTE имеет явно выраженную инновационную направленность. Корпорация ZTE находится среди первых компаний по количеству зарегистрированных патентов. Это позволяет проводить эффективную политику продаж продукции, созданной на базе собственных «ноу-хау». Благодаря высоким надежности и качеству производимой ZTE продукции она составляет технологическую базу как ведущих китайских связных операторов, так и более 500 операторов связи по всему миру.

В России ZTE активно сотрудничает с такими крупными операторами как МТС, Вымпелком, Ростелеком, Мегафон и другими. В настоящий период в рамках углубления российско-китайского сотрудничества корпорация ZTE осуществляет комплекс мер по расширению своего присутствия на российском рынке. Основополагающими принципами, которые лежат в основе указанного курса являются:

- четкое исполнение российского законодательства во всех сферах финансово-экономической деятельности корпорации ZTE в России;
- гибкая партнерская политика корпорации, позволяющая осуществлять свою деятельность в Российской Федерации в различных формах и форматах, учитывающих особенности и интересы российских потребителей, как в центре, так и в регионах;
- поставка российским потребителям доверенного технологического оборудования, производимого корпорацией ZTE и формирование на этой основе устойчивых представлений о корпорации ZTE как надежном партнере;
- гибкая финансовая политика расчетов за поставки, которая предоставляет покупателю несколько вариантов рассрочки платежей.

Такой подход позволяет установить тесное сотрудничество с российскими регуляторами и компаниями, осуществляющими сертификационную и проверочную деятельность оборудования, производимого ZTE. Различные форматы сотрудничества предполагают готовность корпорации ZTE осуществлять локализацию линейки своей продукции под российскими брендами и под заказ российских потребителей. Наличие в структуре учредителей корпорации ZTE крупнейших китайских банков позволяет корпорации реализовывать заказы под рассрочку платежей, что особенно актуально в условиях кризиса.

Очень важным конкурентным преимуществом корпорации ZTE является готовность производить в интересах российских заказчиков доверенное технологическое оборудование, что создает для российской стороны гарантии устойчивого функционирования оборудования корпорации ZTE в любых условиях обстановки.

Отдельной темой является готовность корпорации ZTE предоставлять российским потребителям готовые инновационные решения в сферах управления крупными промышленными предприятиями, на транспорте, в нефтегазовой промышленности, в энергетике, добывающей и обрабатывающей промышленности. Сюда же можно отнести решения по таким сферам как «умный

город», «умный регион», а также собственные разработки средств обеспечения информационной безопасности сложных технологических комплексов. При этом речь идет не о теоретических разработках, а о конкретных технологиях, которые уже реализованы и успешно функционируют как в КНР, так и в ряде зарубежных стран.

Перечисленные направления деятельности ZTE на российском направлении существенно расширят спектр поставляемой в Россию продукции, которая на сегодня представлена в большей степени гаджетами (смартфонами, планшетами, телефонами и т.д.). Кстати, по продажам указанной продукции ZTE занимает 4-ое место в мире.

На основе указанного подхода к организации бизнеса на территории Российской Федерации корпорация ZTE в настоящее время устанавливает взаимодействие с российскими компаниями со смешанным капиталом, такими как ОАО «РЖД», «Газпром», «Роснефть», «Башнефть», «Татнефть», государственной корпорацией Ростехнологии и компаниями, входящими в ее структуры, с крупными российскими системными интеграторами-производителями IT-продукции и средств защиты информации и многими другими российскими структурами и корпорациями. Налаживается сотрудничество с руководителями регионов и находящимися в регионах профильными предприятиями.

Руководство корпорации ZTE, ее ученые и сотрудники разделяют озабоченности международного сообщества в связи с ростом угроз кибертерроризма и кибервойн. В своей деятельности корпорация ZTE стремится содействовать укреплению мер доверия со своими партнерами и одновременно готово своими решениями содействовать укреплению международной безопасности.

Мы надеемся, что через возможности настоящего Форума корпорация ZTE совместно с заинтересованными партнерами внесет свой посильный вклад как в укрепление российско-китайского сотрудничества, так и в укрепление международной информационной безопасности.

В заключение хотел бы пожелать всем участникам реализации планов и замыслов, направленных на снижение угроз злонамеренного использования глобального информационного пространства и мирного неба над головой.

S.V.Ustyugov
ZTE Corp. (China)

The main priorities of ZTE Corporation for entering the Russian market and promotion of international information security

In my presentation I would like to stress the importance of the Forum from the standpoint of ZTE Corporation, say a few words about the current position of ZTE Corporation in the global telecommunications market, as well as the basic principles and directions of its work in Russia.

First of all, let me extend greetings to the organizers and participants of the Forum on behalf of the President of ZTE Corporation Mr. Shi Lirong, the leadership of the Russian Directorate of ZTE Corporation, on my own behalf and wish you all success, health and well-being. We also express our gratitude for the invitation to take part in the Ninth International Forum «Partnership of State Authorities, Civil Society and the Business Community in Ensuring International Information Security».

Over the last years, the Forum has evolved into an important tool for consolidating the efforts of IT-specialists of many countries in countering the threats of cyberterrorism and cyberwar. Essentially, thanks to the Forum, in which we can see participation of the leading experts and scientists of interested countries, a new universal human value has been formed — a system of international information security. Its main value is determined by a set of rules for the use of information and communication networks and by a set of evaluation criteria for actions of subjects of global communication.

This assessment of significance of the Forum allows for a number of analogies. For example, no one doubts the importance for any community to have a Constitution — the basic law by which it lives. It allows the community to qualify the good and the bad, to accept the rules of the Law, which define the responsibility of citizens for their actions. However, at the moment there are no such rules in the global cyberspace.

In this regard, it is fair to say that specialists from many countries and their efforts in the framework of the Forum are forming a certain prototype of the Universal Law of the Internet, which in addition to determining the rules of conduct and responsibility of subjects of global

communications, would promote cooperation between different countries on the basis of shaping of a trusted information environment.

This is particularly true in the context when information sphere is being used by individual nation-states to toughen dictate with regard to both its partners and allies, and to countries, which wish to pursue independent policy. Therefore today, both political and technological solutions to ensure international information security are in great demand by many members of the international community. It is known that it is easier to endure difficult circumstances with joint efforts of partners.

Under these conditions, the relations between the Russian Federation and the People's Republic of China began to take shape of a strategic partnership. ZTE Corporation is among the companies that seek to contribute to the strengthening of Russian-Chinese cooperation through an increased interaction with Russian consumers of high-tech products.

The presence in the Russian market and the strategy of ZTE Corporation in Russia has not been widely covered by the media. Therefore, I would like to say a few words about ZTE Corporation. It was founded in 1985. By the form of enterprise, ZTE is a joint stock company with majority interest being held by Chinese Aerospace Corporation, which is public. ZTE is one of the largest manufacturers of telecommunications equipment not only in China but throughout the world. The branches of the Corporation are present in more than 100 countries. There are 18 research centers which successfully operate in China and abroad. The work of ZTE Corporation has a pronounced forward-thinking orientation. ZTE Corporation is among the leading companies by the number of registered patents. This allows for an effective policy of sales of products created on the basis of proprietary «know-how». High reliability and quality of manufactured products, allows them to serve as a technological base of the leading Chinese communications service provider and more than 500 communications service providers worldwide.

In Russia, ZTE is actively cooperating with major mobile network operators, such as MTS, VimpelCom, Rostelecom, Megafon and others. Currently, with the deepening of Russian-Chinese cooperation, ZTE is implementing a set of measures to expand its presence in the Russian market. The fundamental principles that lie at the heart of this strategy are:

- accurate execution of the Laws of the Russian Federation in all spheres of financial and economic activity of ZTE Corporation in Russia;
- flexible partnership policy of the Corporation, which allows it to work in the Russian Federation in various forms and formats, taking

into account the qualities and interests of Russian consumers, both in central regions and throughout the country;

- supply of trusted technological equipment produced by ZTE Corporation to Russian consumers and formation on this basis of a sustainable perception of ZTE Corporation as a reliable partner;
- flexible financial settlement policy, which gives the customer several options for payment by installments.

This approach allows us to establish close cooperation with the Russian regulators and companies engaged in certification and verification of equipment produced by ZTE. Different forms of cooperation involve the willingness of ZTE Corporation to localize its product lineup under Russian brands and customized for Russian consumers. The presence of China's largest banks in the founding structure of ZTE Corporation allows the Corporation to fulfill orders for payment by installments, which is especially important in times of crisis.

The willingness of ZTE Corporation to produce trusted technological equipment in the interests of Russian customers is an important competitive advantage and guarantees for the Russian side a stable operation of ZTE Corporation equipment in any situation.

A separate topic is the willingness of ZTE Corporation to provide Russian consumers with innovative out-of-the-box solutions in management of large industrial enterprises, transport, oil and gas, energy, mining and manufacturing industries. This category can also include such solutions as «smart city», «intelligent region», as well as proprietary information security solutions for advanced technological complexes. This being said, we are not talking about theoretical developments, but about specific technologies that have already been implemented and successfully operate both in China and abroad.

This business profile of ZTE Corporation in Russia will significantly expand the range of products supplied to Russia, which is now to a greater extent represented by gadgets (smartphones, tablets, phones, etc.). At that, ZTE ranks fourth in the world by sales of the abovementioned products.

On the basis of this approach to business organization on the territory of the Russian Federation, ZTE is currently establishing cooperation with Russian mixed capital companies such as JSC «Russian Railways», «Gazprom», «Rosneft», «Bashneft», «Tatneft», Russian Technologies State Corporation and its affiliated companies, with major Russian system integrators-manufacturers of IT-products and information security solutions and many other Russian institutions and corporations. Cooperation is being established with the heads of the regions and regional core enterprises.

The leadership of ZTE Corporation, its scientists and staff members share the concern of the international community over the growing threat of cyberterrorism and cyberwarfare. In its activities, ZTE Corporation seeks to promote confidence-building measures with its partners and at the same time is ready to contribute with its solutions to the strengthening of international security.

We hope that through this Forum ZTE Corporation together with interested partners will make a fair share of contribution to strengthening of Russian-Chinese cooperation, and to strengthening of international information security.

In conclusion I would like to wish all the participants peaceful skies and implementation of their plans and designs aimed at reducing the threat of malicious use of global information space.

Е.Г.Голомазов, И.В.Зимин

Институт электроники и телекоммуникаций при Кыргызском государственном техническом университете им. И. Раззакова

Проблемы и особенности информационной безопасности в Кыргызской республике

Информационная сфера является ключевой сферой жизни Кыргызстана, как государства и как целостного в своем разнообразии общества.

В последнее время вопрос информационной безопасности Кыргызстана (Киргизии) очень часто становится предметом дискуссии и споров. И чаще всего со ссылкой на некие информационные войны, сопровождавшие последние политические события и социальные потрясения.

17 июня 2015 года в какой-то мере является знаковой чертой, которая определит будущее нашего информационного пространства и нашей представленности в цифровых пакетах вещания. Госпрограмма по переходу на цифровое вещание предусматривает лишь выполнение технических обязательств по международному соглашению «Женева — 06». Что будет вещать оператор, получивший цифровые частоты — об этом пока еще никто не думал. Важность информационного ресурса для государства определяется контентом, который получает потребитель, являющийся гражданином страны. И для государства важно позаботиться, чтобы в этих пакетах было больше местных СМИ, освещающих события и государственную политику страны. Сегодня в этом плане картина выглядит удручающей.

В Бишкеке из 18 каналов, вещающих в открытом формате, 14 почти полностью ретранслируют зарубежные программы ОРТ, РТР, Вести-24, Культура, НТВ, СТС, ТНТ, Рен-ТВ, Мир, MTV, КТК, Эл-Арна, Хабар, CCTV. Местных каналов всего четыре — ОТРК, ЭлТР, 5-й канал, Эхо Манаса.

Не менее плачевна ситуация на юге страны. На территорию страны свободно вещают тринадцать узбекских и пять таджикских каналов. А ведь есть еще и радиостанции.

Почему сложилась такая картина? Есть две основные причины — политическая и техническая. Примерно с 2001 года выдача частот под телерадиовещание превратилась в процедуру, которая заведомо играла против информационной безопасности Кыр-

гызстана. Более 60-ти заявителей до сих пор стоят в очереди на частотное присвоение, надеясь, что когда-нибудь всё же смогут открыть свой канал. Но *политика государства* того времени оказалась незаинтересованной в честном развитии частного медиарынка. Выдача частот официально прекратилась, хотя новые каналы все же появлялись.

СМИ, освещающие местные события, постепенно превращались в инструмент информационного влияния. Остальные вещатели решили не связываться с политикой, и перешли на ретрансляцию.

Вторая причина — сложность географического рельефа. Он не позволяет эффективно использовать имеющиеся частотные ресурсы. Для их освоения приходится строить больше станций, дублировать один и тот же канал в разных регионах на разных частотах, тратить больше денег на поддержание существующего вещания.

В свое время в надежде развить вещание многие столичные телерадиокомпании получили в регионах определенное количество частот. Но из-за дороговизны построения собственных сетей, неразвитости рынка рекламы, ограниченности существующих каналов релейной подачи сигнала — они их до сих пор не запустили.

Сегодня же этот вопрос по-прежнему не решается. Но уже под официальным предлогом того, что грядет цифровой век и выдача аналоговых частот нерентабельна, так как вещание в аналоговом режиме после 2015 года всё равно придется прекращать.

В разных регионах Кыргызстана планируется запустить от 10 и более мультиплексов. В некоторых регионах их будет свыше 30-ти, если туда пойдут операторы связи. Согласно госпрограмме государство берет на себя заботу лишь о социальном пакете, куда войдут вещатели, финансируемые из бюджета. Их не так много — 3–5 каналов республиканского масштаба. Плюс в каждой области еще по одной телестанции. А вместить в оплаченный государством мультиплекс можно до 14(!) каналов. Что делать с остальным пространством? Забота государства заключается в построении собственного мультиплекса и обеспечении его развития до каждого отдаленного уголка страны.

Телевидение в Кыргызстане является одной из основных составляющих СМИ. Так называемая Арабская весна, смысловые противостояния между сторонниками европейского и евразийского пути развития на пространстве бывшего СССР, цивили-

зационные, культурные и межконфессиональные противоречия демонстрируют новые возможности современного информационного взаимодействия или противодействия. Кыргызстан за последние пять лет испытал целый ряд прямых информационных атак, существенно повлиявших на общественно-политическую ситуацию в стране. Сегодня, даже находясь на периферии мировой турбулентности, страна, так или иначе, вовлечена в глобальные информационные противостояния. Манипулятивные технологии, зачастую используемые внешними игроками для иных целей и территорий, тем не менее оказывают симметричный эффект на Кыргызстан. Но наиболее высоким риском является тенденция к потере субъектности государственных и гражданских институтов, участников рынка, размывание гражданской, ментально-культурной общностей. Государство теряет свой базовый иммунитет. Это прямая угроза суверенитету Кыргызской Республики. Опасность в том, что пока нет прямых внешних агрессий против Кыргызстана, все эти явления носят скрытый, бессимптомный характер. Но это не отменяет их деструктивных последствий. Однако, как показывает мировая практика, стремление закрыть или ограничить национальное информационное пространство, установить в нем жесткий контроль малоэффективно и несет новые риски.

В национальном информационном пространстве присутствуют зарубежные СМИ, которые нередко имеют преимущество над кыргызскими СМИ. Так, кыргызские СМИ не занимаются страновым позиционированием в региональном и глобальном пространстве: отсутствие собственных качественных международных новостей для освещения мировых событий и процессов привело к тому, что представления кыргызского общества о мировых процессах и собственное позиционирование по отношению к ним формируют иностранные СМИ или кыргызские СМИ, работающие в рамках иностранных информационных дискурсов, что приводит к абсолютной неадекватности к своему местоположению, задачам и целям. Более того, равнозначное присутствие на национальном поле иностранных СМИ не просто включает их во внутреннюю информационную конкуренцию, но и подменяет национальную повестку, отвлекая от насущных проблем. Это размывает и разрушает субъектность государственных и общественных институтов. Информационно Кыргызстан продолжает находиться в пределах постсоветского информационного пространства.

Миссией Концепции информационной политики является укрепление суверенитета и государственной безопасности Кыргызской Республики, создание условий для устойчивого развития Кыргызстана, укрепление и развитие демократических гражданских и государственных институтов. Информационная политика Кыргызстана должна создать условия для эффективного использования гражданами и государством возможностей странового и глобального информационных пространств.

Комплекс действий в сфере информационной безопасности преследует несколько долгосрочных целей:

- укрепление информационного суверенитета Кыргызстана наряду с открытостью к процессам информационной глобализации;
- поддержание постоянного открытого и конструктивного диалога всех субъектов общества и государства с целью устойчивого развития Кыргызстана;
- уменьшение уязвимости кыргызстанского общества к внутренним конфликтам, способствование примирению, мирному сосущест-вованию, укрепление общественного, межнационального и межконфессионального согласия, предупреждение конфликтогенности;
- сохранение и развитие единого национального информационного и культурного поля для формирования общенациональных смыслов, идентифицирующих и позиционирующих Кыргызстан как суверенное государство;
- укрепление институтов (норм, процедур, надзора) информационной безопасности Кыргызской Республики;
- повышение готовности Кыргызской Республики к противодействию в кризисных ситуациях;
- сохранение и утверждение демократических ценностей вне зависимости от технологических вызовов информационной среды.

В политике информационной безопасности применяется общий принцип ориентированности на предотвращение конфликтов и повышение безопасности за счет законности, открытости, равной ответственности всех сторон информационного взаимодействия перед законом. Государство в сотрудничестве с гражданским обществом и международными институциями обеспечивает постоянный мониторинг проявлений ненависти и разжигания вражды в информационной сфере, правоохранительная система пресекает эти проявления в рамках закона.

Технологическая революция позволяет создать новый дискурс вокруг новых интернет-базированных информационных каналов, доступных для молодой аудитории, продвигающийся по мере смещения демографических границ. Изменение способа потребления медиа облегчает задачу модифицирования информационного дискурса. В сфере социальных сетей и интерактивного сегмента Интернета важно формирование противодействия системам политического троллинга. Игровая механика (gamification) и фактор влияния со стороны сверстников могут быть задействованы в катализации процесса формирования субъектности молодого поколения.

Наличие нефильтрованного Интернет-трафика позволяет иметь постоянный доступ к различным источникам информации. Наличие доступа будет результативным фактором безопасности, если совместится с высоким уровнем медиа-грамотности, критическим мышлением и наличием структурированного медиапространства с ключевой ролью общественного вещания.

Массовое развитие навыков программирования, развитие рынка программирования и глобальная интегрированность кыргызстанского рынка производства программного обеспечения делает возможным более безопасное использование решений на основе так называемого «открытого кода» наряду с использованием «закрытого кода». Это позволяет сделать онлайн-ресурсы Кыргызстана более устойчивыми и защищенными от внешнего воздействия.

Государство создает условия для защиты данных, создавая стандарты. Операторы и собственники баз данных всех форм собственности формируют на основе стандартов механизмы защиты данных.

Грамотная и последовательная политика в сфере информационной безопасности является прямым условием суверенитета и целостности государства.

E.G.Golomazov, I.V.Zimin
Institute of Electronics and Telecommunication Kyrgyz State Technical University (the Republic of Kyrgyzstan)

Issues and special aspects of information security in the Kyrgyz Republic

The information sphere is a key area of life in Kyrgyzstan, as a state and as a society coherent in its diversity.

The issue of information security in Kyrgyzstan has recently become a frequent subject of discussion and controversy. And more often than not with the reference to some information wars that accompanied the recent political developments and social upheaval.

June 17 of 2015 will be, to some extent, a significant milestone that will determine the future of our information space, and our representation in digital broadcasting packages. The State program for transition to digital broadcasting provides only for compliance with the technical obligations under an international agreement «Geneva-06». What will be broadcast by the operator, who obtains digital frequencies — no one has thought of it yet. The importance of an information resource for the nation-state is determined by the content received by consumer, who is a citizen of the country. And it is important for the government to make sure that these packages include more of the local media, which cover events and the state policy of the country. Today, in this respect, the picture looks depressing.

In Bishkek, 14 out of 18 channels broadcasting in an open format almost completely rebroadcast foreign programs of ORT, RTR, Vesti-24, Culture, NTV, STS, TNT, REN-TV, MIR, MTV, STS, El Arna, Khabar, CCTV. There are only four local channels — PTRC, ElTR, Channel 5, Echo of Manas.

Equally deplorable is the situation in the south of the country. Thirteen Uzbek and five Tajik channels freely broadcast on the territory of the country. And then there are also radio stations.

Why can we observe such a picture? There are two main reasons — political and technical. Since around 2001, the allocation of broadcasting frequencies has become a routine that obviously played against information security of Kyrgyzstan. More than 60 applicants are still

in the line for frequency allocation, hoping that someday they still will be able to open their own channel. But the *policy of the state* at the time turned out to be uninterested in fair development of the private media market. Frequencies allocation had officially ended, although new channels still continued to appear.

Local media gradually transformed into a tool of information influence. The rest of the broadcasters decided not to get involved with politics and turned to rebroadcasting.

The second reason — is the complexity of geographical terrain. It does not allow the efficient use of available frequency spectrum. For its development it is necessary to build more stations, duplicate the same channel in different regions at different frequencies, and spend more money to maintain existing broadcasting.

At the time, in hope of developing broadcasting, many metropolitan television and radio broadcasting company received certain bandwidths in the regions. But because of the high cost of building their own networks, weak advertising market, limits of existing relay signal lines — they have not launched them yet.

Today this issue is still not being solved — but under the official pretext that we are on the verge of a digital age and issuance of analog frequencies is unprofitable, as analog broadcasting will have to stop after 2015 anyway.

It is planned to launch 10 or more multiplexes in each region of Kyrgyzstan. In some regions there will be over 30, if communication providers will participate. According to the state program the government takes care only of the social package, which will include broadcasters that are financed from the budget. There are not so many of them — 3–5 channels of republican scale. And an extra TV station in each region. And it is possible to accommodate up to 14 (!) channels in the state-paid multiplex. What is to be done with the rest of the bandwidth? The concern of the State is to build its own multiplex and ensure its development in every remote area of the country.

Television in Kyrgyzstan is one of the main components of media. The so-called Arab Spring, semantic confrontation between the supporters of European and Eurasian path of development in the territory of the former USSR, civilizational, cultural and inter-religious contradictions demonstrate the new possibilities of modern information interaction and counteraction. Over the past five years Kyrgyzstan has experienced a number of direct information attacks, which greatly in-

fluenced the socio-political environment of the country. Today, even being on the periphery of the global turbulence, the country is one way or another involved in the global information confrontations. Manipulative techniques which are often used by external actors for other purposes and territories nevertheless have a symmetrical effect on Kyrgyzstan. But the greatest risk is the tendency to loss of subjectivity of state and civil institutions, market players, erosion of civil and mental-cultural communities. The nation-state loses its basic immunity. This is a direct threat to the sovereignty of the Kyrgyz Republic. The danger lies in that, while there is no direct external aggression against Kyrgyzstan, all these phenomena are of concealed and asymptomatic nature. But this does not negate their destructive effects. However, the world practice shows, that the ambition to close or restrict national information space or to impose strict control is ineffective and carries new risks.

The foreign media that is present in national information space often has an advantage over the Kyrgyz media. For instance, Kyrgyz media do not engage in country positioning in regional and global space: the absence of indigenous high-quality international news for coverage of global events and processes has led to the fact that perception and views of Kyrgyz society on the global processes are being formed by the foreign media or the Kyrgyz media, working within the framework of foreign information narratives. This leads to absolute inadequacy of the views and perception with regard to place, goals and objectives. Moreover, the equal presence of the foreign media in the national space does not just include them into the inner informational competition, but also substitutes national agenda and distracts from the current issues. It dilutes and disrupts subjectivity of the state and public institutions. Information-wise Kyrgyzstan continues to be within the post-Soviet information space.

Objectives and Means of information security

The goal of the Concept of Information Policy is to strengthen the sovereignty and national security of the Kyrgyz Republic, to create conditions for sustainable development of Kyrgyzstan, strengthening and development of democratic civil and state institutions. Information policy of Kyrgyzstan must provide conditions for effective use of national and global information space by the citizens and the state.

The set of measures in the field of information security has several long-term goals:

- strengthening of information sovereignty of Kyrgyzstan, along with openness to the processes of information globalization;
- maintain a constant open and constructive dialogue between all actors of the society and the State for the purpose of sustainable development of Kyrgyzstan;
- reduce the vulnerability of Kyrgyz society to internal conflicts, promote reconciliation, peaceful coexistence, strengthening of social, ethnic and interreligious understanding, prevention of conflictogenity;
- preservation and development of a unified national information and cultural space to shape national values which identify and position Kyrgyzstan as a sovereign state;
- strengthening of information security institutions (rules, procedures, supervision) of the Kyrgyz Republic;
- increase the preparedness of the Kyrgyz Republic to counter crisis situations;
- preservation and strengthening of democratic values, regardless of technological challenges of the information environment.

Information security policy uses the general principle of orientation on conflict prevention and improving of security through the rule of law, openness, and equal amenability of all parties of information exchange. The government in collaboration with civil society and international institutions ensures constant monitoring of information sphere for manifestation and incitement of hatred, and the law enforcement system precludes these manifestations within the Law.

The technological revolution makes it possible to create a new narrative around new Internet-based information channels available to a younger audience, which advances with the demographic boundaries. Change in means of media consumption makes it easier to modify the information narrative. With regard to social networking and interactive segment of the Internet it is important to develop a response to the systems of political trolling. Game mechanics (gamification) and the factor of peer influence can be involved in the process of catalyzing the formation of subjectivity of the younger generation.

Availability of unfiltered Internet traffic enables instant access to the various sources of information. Availability of access can be an effective safety factor if it is combined with a high level of media literacy,

critical thinking and the presence of a structured media space with the key role of public broadcasting service.

Wide-scale development of programming skills, development of software engineering market and global integration of Kyrgyz software market provides for a more secure use of so-called «open source» solutions in comparison with «closed source» solutions. This allows making online resources of Kyrgyzstan more stable and protected from external influences.

The nation-state creates conditions for data protection by introducing standards. Operators and owners of databases with all forms of ownership develop standards-based data protection mechanisms.

Appropriate and consistent policy in the field of information security is a straightforward prerequisite for sovereignty and integrity of the nation-state.

Ninth International Forum «Partnership of State Authorities, Civil Society and the Business Community in Ensuring International Information Security» and Eleventh Scientific Conference of the International Information Security Research Consortium April 20–23, 2015. Garmisch-Partenkirchen, Munich, Germany, 2015. — Moscow: Moscow University Press, 2015. — 288 p.

The proceedings of the Ninth International Forum «Partnership of State Authorities, Civil Society and the Business Community in Ensuring International Information Security» and the Eleventh Scientific Conference of the International Information Security Research Consortium include reports by leading domestic and foreign experts engaged in research of Information security, Cybersecurity and International Information security.

Key words: Information security, Cybersecurity, International Information security, Critical Infrastructure protection, International Law, International Humanitarian Law, Cyberconflicts, Cyberwar.

Научное издание

Девятый международный форум
«Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности»
и Одиннадцатая научная конференция Международного исследовательского консорциума информационной безопасности
20–23 апреля 2015 года.
Гармиш-Партенкирхен, Германия

Текст публикуется в авторской редакции
с оригинал-макета, представленного заказчиком

Подписано в печать 31.10.2015. Формат $60\times90^{1}/_{16}$.
Бумага офсетная. Офсетная печать.
Гарнитура Ньютон. Усл. печ. л. 22,0.
Уч.-изд. л. 14,93.
Тираж 200 экз. Изд. № 00 000. Заказ №

Издательство Московского университета.
125009, Москва, ул. Б. Никитская, 5.
Тел.: (495) 629-50-91. *Факс:* (495) 697-66-71.
Тел.: (495) 939-33-23 (*отдел реализации*).
E-mail: secretary-msu-press@yandex.ru

Сайт Издательства МГУ:
www.msu.ru/depts/MSUPubl2005
Интернет-магазин: http://msupublishing.ru

Адрес отдела реализации:
Москва, ул. Хохлова, 11 (Воробьевы горы, МГУ).
E-mail: izd-mgu@yandex.ru. *Тел.:* (495) 939-34-93