Издательство московского университета
2014

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

Ninth Scientific Conference of the International Information Security Research Consortium

April 21–24, 2014
Garmisch-Partenkirchen, Munich, Germany

Восьмой международный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности»

Девятая научная конференция Международного исследовательского консорциума информационной безопасности

21–24 апреля 2014 года
Гармиш-Партенкирхен, Германия

ОАО «НИИАС» РЖД

ICANN

УДК 327;930.22;007
ББК 66.4;73
В78

Восьмой международный форум «Партнерство государ-
В78 ства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» и Девятая научная конференция Международного исследовательского консорциума информационной безопасности 21–24 апреля 2014 года. Гармиш-Партенкирхен, Германия. — М.: Издательство Московского университета, 2014. — 288 с.

ISBN 978-5-19-011008-1

В настоящем сборнике материалов Восьмого международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» и Девятой 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 978-5-19-011008-1

Содержание

В.П.Шерстюк. Вступительное слово: О программе и задачах Форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» 8

V.P.Sherstyuk. Opening Remarks: On Agenda and Challenges of the Forum «State, Civil Society and Business Partnership on International Information Security 14

С.М.Бураулев. Приветствие к организаторам, участникам и гостям Восьмого международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» 19

S.M.Buravlev. Welcome Address to organizers, participants and guests of the VIII International Forum «State, Civil Society and Business Partnership on International Information Security» 22

Чарльз Барри (*Charles Barry*). Вызовы защиты критически важной инфраструктуры: Надежность систем в цифровой век 25

Dr. Charles (*Chuck*) *Barry*. Challenges in the Protection of Critical InfrastructureSystems Reliability in the Digital Age 40

А.А.Стрельцов. Основные направления развития международного права вооруженных конфликтов применительно к киберпространству 52

Dr. A.A.Streltsov. Focal Areas in Development of International Law of Armed Conflict in the Context of Cyberspace 62

Гао Хуэй (*Gao Hui*). Применимость права вооруженного конфликта в киберпространстве 71

Gao Hui. Applicability of the Law of Armed Conflict in Cyberspace . 75

И.Н.Дылевский, В.О.Запивахин, С.А.Комов, А.Н.Петрунин. Об адаптации международно-правового понятия «агрессия» к специфике информационного пространства 79

I.N.Dylevskiy, V.O.Zapivakhin, S.A.Komov, A.N.Petrunin. Adaptation of international legal concept of “aggression” to the specifics of information space 91

Н.В.Соколова. О международно-правовых аспектах использования информационно-коммуникационных технологий: опыт Группы правительственных экспертов ООН по международной информационной безопасности 101

N.V.Sokolova. On international legal aspects of the use of information and communication technologies: the experience of the UN Group of Governmental Experts on international information security 107

Сюй Люнди (*Xu Longdi*). Факторы, оказывающие влияние на содержание понятия «Кибервойна» 113

Xu Longdi. Factors Influencing the Definition of 'Cyber Warfare' 118

П.Л.Пилюгин. Проблемы создания технических средств контроля за соблюдением разрабатываемых норм международного права для киберпространства 122

P.L.Pilyugin. Challenges of creating the technical control means for observance of future international law norms for cyberspace 134

Лоран Жизель (*Laurent Gisel*). Как международное гуманитарное право налагает ограничения на ведение кибервойны и предоставляет защиту гражданским лицам? 144

Laurent Gisel. How does international humanitarian law constrain cyber warfare and protect civilians? 156

Пал Вранге (*Pal Wrange*) Международное право и вмешательство в национальное и частное киберпространство 166

Pål Wrange. Intervention in national and private cyberspace and international law 173

Санджай Гоел (*Sanjay Goel*). Адаптация международного права к конфликтам в киберпространстве 179

Sanjay Goel (*Sandro Bologna*) Adaptation of International Law to Cyber Conflict 188

Сандро Болонья (*Sandro Bologna*) Кибербезопасность и устойчивость промышленных систем управления 195

Dr. Sandro Bologna. Cyber Security and Resilience of Industrial Control Systems 207

А.Н.Курбацкий. Личная информационная безопасность и правила поведения в виртуальном пространстве 218

A.N.Kurbatskiy. Personal information security and the rules of conduct in information space 225

Кеир Гилс (*Keir Giles*) Легитимизация онлайн-слежки и мониторинга 231

Keir Giles. Legitimation of Online Surveillance and Monitoring 240

Йоко Нитта (*Yoko Nitta*). Подходы Японии к кибербезопасности Как реагировать на неопределенность? 248

Yoko Nitta. Japan's Approaches towards Cybersecurity 258

Масаеси Кубоя (*Masayoshi Kuboya*). Доверие к киберпространству в Японии:Информационная грамотность и регулирование 266

Dr. Masayoshi Kuboya. Cyberspace Credibility in Japan:Information Literacy and Regulation 272
Н.П.Варновский, О.А.Логачев, В.В.Ященко. Математика и информационная безопасность 277
N.P.Varnovskiy, O.A.Logachev, V.V.Yashchenko. Mathematics and Information Security 282

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 Форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности»

Уважаемые участники конференции!

Дамы и господа!

Прежде всего, хотел бы высказать искреннюю признательность руководителям администрации этого удивительного места в Баварии — г.Гармиш-Партенкирхен, благодаря радушию которых эксперты в области информационной безопасности многих государств мира уже восьмой год подряд могут собираться и обсуждать наиболее актуальные проблемы обеспечения международного мира и безопасности в условиях угроз злонамеренного использования информационных и коммуникационных технологий (ИКТ). Плодотворность этих дискуссий существенно возросла после образования здесь же в г.Гармиш-Партенкирхен Международного исследовательского консорциума, который позволил создать условия для объединения усилий заинтересованных организаций в поиске непростых решений проблем обеспечения международной информационной безопасности.

На предыдущей конференции в Баку в октябре прошлого года Консорциум определил в качестве приоритетного направления своих исследований проработку проблем совершенствования международного права с учетом необходимости противодействия злонамеренному использованию ИКТ в военно-политических целях. Сегодня состоится семинар-круглый стол по этой теме. Завтра состоится IX-ая конференция Консорциума, на которой нам предстоит подвести промежуточные итоги проработки данного вопроса и определиться с планами работы Консорциума на ближайшее будущее. Кроме того, состоится прием в организацию новых членов. Это:

Научно-исследовательский институт информационной безопасности и криптологии Евразийского национального университета им. Л.Н.Гумилева (Казахстан);
Институт электроники и телекоммуникаций при Кыргызском государственном техническом Университете им. И. Раззакова (Кыргызстан).

В развитие решений Консорциума за время, прошедшее с нашей последней встречи в г. Гармиш-Партенкирхен в 2013 г., проделана большая работа.

Мы приняли участие в пленарном заседании Европейского Альпбахского Форума (Австрия) на тему «Кибервойна — взгляды и подходы основных участников», где поддержали идею активизации усилий по совершенствованию международного права, регулирующего международные отношения в области противодействия военному использованию ИКТ.

По аналогичной теме в апреле в г. Стокгольме (Швеция) на базе российского посольства проведена российско-шведская встреча экспертов (семинар) по международной информационной безопасности. В рамках встречи затрагивались также вопросы реализации прав и свобод человека в сети Интернет.

В конце октября — начале ноября 2013 года в г. Нью-Йорк (США) проведена тематическая встреча ученых в формате международного семинара «Управление Интернетом и киберконфликты: модели, регулирование и меры укрепления доверия». Американская сторона выступила с инициативой проводить подобные встречи ученых и экспертов по «сверке часов» ежегодно.

Кроме того, эксперты МГУ приняли участие в конференции «Международное сотрудничество в киберпространстве» (Джорджтаунский университет, г. Вашингтон, США), IV Всемирном саммите по кибербезопасности (Стэнфорд, США), в конференции «Национальная безопасность и развитие науки и техники» (г. Чанша, КНР), Первой международной научно-практической конференции «Информационная безопасность в свете Стратегии Казахстан — 2050» (г. Астана, Казахстан), в конференции «Власть и бизнес в эпоху Интернета» (г. Лондон, Великобритания).

На нашу Конференцию вынесены весьма важные и сложные вопросы формирования системы международной информационной безопасности, способной снизить опасность использования ИКТ для нарушения международного мира и безопасности.

Во-первых, проблемы адаптации международного права к конфликтам в информационном пространстве. В рамках обсуждения данного вопроса на «круглом столе» предполагается обсудить:

- содержание понятия «атака» в информационном пространстве;
- применение принципов разграничения, пропорциональности и мер предосторожности в конфликтах с использованием ИКТ;
- право нейтралитета в конфликтах с использованием ИКТ;
- содержание понятий «сила» и «угроза силой или применения силы» в информационном пространстве;
- содержание понятий «вооруженное нападение» и «агрессия» в информационном пространстве;
- организацию атрибуции фактов применения силы на основе злонамеренного использования информационных и коммуникационных технологий.

По поводу почти каждого из выделенных вопросов опубликовано значительное количество работ, но искомое решение, как нам представляется, еще не найдено.

Данное обстоятельство отчасти объясняется тем, что рассматриваемая проблема связана не столько с пробелами или противоречиями в действующем законодательстве, сколько с неопределенностью трактовок существующих норм международного права применительно к условиям киберпространства, т.е. с необходимостью адаптации правовых норм к новым условиям применения.

В основу решения задачи предлагается положить концепцию «неявного оружия». Ее существо заключается в том, что в определенных случаях злонамеренное использование ИКТ придает свойства «оружия», т.е. средств и механизмов, предназначенных для поражения живой силы и техники, объектам невоенного назначения, например, гражданским самолетам, атомным электростанциям и т.п. Данная концепция позволяет выявить достаточно четкие признаки использования ИКТ в качестве оружия и, соответственно, условия, при которых злонамеренное использование ИКТ может рассматриваться как вооруженное нападение, порождающее у государства–жертвы неотъемлемое право на индивидуальную или коллективную самооборону. Одновременно появляется возможность более четко определить те нормы международного права применения силы и международного гуманитарного права, которые требуют адаптации к условиям злонамеренного использования ИКТ.

Второй важной проблемой противодействия угрозам международного мира и безопасности в киберпространстве является обеспечение информационной безопасности критически важных инфраструктур. Обсуждению этой проблемы также будет посвящен отдельный «круглый стол».

В рамках его работы предполагается рассмотреть вопросы:

- сравнительного анализа подходов различных стран по отнесению отдельных сегментов информационной инфраструктуры к категории критически важных;
- передовых практик использования частно-государственного партнерства в области обеспечения информационной безопасности критически важных инфраструктур;
- маркировки и идентификации информационных систем и сетей, защищенных международным правом, в киберпространстве;
- создания международной системы мониторинга и объективизации нарушений норм международного права в отношении информационных систем и сетей.

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, касающихся защиты жертв международных вооруженных конфликтов, 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 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 конференции, является сравнительный анализ национальных подходов и приоритетов в области формиро-

вания системы международной информационной безопасности.

В рамках работы соответствующего «круглого стола» предполагается обсудить вопросы:

- легитимизации наблюдения и контроля в сетях;
- реализации национальных информационных стратегий;
- национального опыта противодействия киберпреступности;
- технической разведки в сетях связи в контексте защиты прав человека;
- международных и национальных подходов к противодействию использованию Интернета в террористических и экстремистских целях;
- обеспечения доверия в киберпространстве.

Мы понимаем, что каждый из выделенных вопросов 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 соответствующих проблем.

Наконец, четвертой проблемой, вынесенной на обсуждение участников конференции, являются технологические аспекты обеспечения международной информационной безопасности, базирующиеся на новых перспективных разработках.

В рамках данной проблемы предполагается обсудить вопросы:

- агрегации, интеграции и обеспечения безопасности больших массивов данные в науках о жизни и медицине;
- слияния био- и нанотехнологий: последствия и влияние на информационную безопасность;
- применения достижений математических наук для решения задач обеспечения информационной безопасности.

По существу, в рамках данного «круглого стола» будут анализироваться факторы, определяющие как настоящее, так и будущее проблематики международной информационной безопасности.

Наша конференция проходит в преддверии начала работы очередной Группы правительственных экспертов ООН по международной информационной безопасности (2014–2015 гг.), которой Генеральной ассамблеей ООН поручено продолжить исследования в рассматриваемой области. Пред-

ставляется, что наши дискуссии в определённой мере явятся этапом в подготовке к данному событию.

В заключение доклада хочу сообщить, что в работе конференции принимает участие около 100 ученых и специалистов из 21 государства мира (Россия, США, Китай, Великобритания, Франция, Германия, Япония, Австралия, Австрия, Азербайджан, Бахрейн, Белоруссия, Болгария, Израиль, Италия, Казахстан, Камбоджа, Канада, Киргизия, ОАЭ, Швейцария), а также представители 3 международных организаций (Международный комитет красного креста, ICANN (Международная корпорация по присвоению доменных имен и номеров), Европейский центр оборонных исследований и технологий).

Подготовка и проведение такой представительной конференции были бы невозможны без помощи организаций — спонсоров, представители которых присутствуют в зале.

Я хотел бы перечислить их.

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

Огромное им 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 Forum «State, Civil Society and Business Partnership on International Information Security

Dear participants of the conference!
Ladies and gentlemen!

First of all, I would like to express my sincere gratitude to the leadership of the local administration, of this amazing place in Bavaria — Garmish-Partenkirchen. By virtue of their hospitality, information security experts from many countries are able to get together in this place for eighth consecutive year and discuss the most current issues of international peace and security in the context of threats of information and communication technologies misuse. The fruitfulness of these discussions significantly increased after International Research Consortium has been formed here in Garmish-Partenkirchen. It enabled the conditions to combine the efforts of stakeholders in finding complex solutions to the issues of international information security.

In the course of the previous Conference, which took place in Baku in October last year, the Consortium has identified a priority research venue. Taking into consideration the need to counter malicious use of ICTs for military-political purposes, the research is focused on elaboration of international law improvement issues. Today there will be a workshop-round table on this topic. The IX International Conference of the Consortium will take place tomorrow. In its course we will summarize the interim results of this research and decide on plans of the Consortium for the near future. In addition, new members will be admitted to the Consortium. They are:

- Institute of Information Security and Cryptology (IIS&C) at the Gumilyov Eurasian National University (Kazakhstan);
- Institute of Electronics and Telecommunications under Kyrgyz State Technical University (Kyrgyzstan).

As a follow-up to the decisions of the Consortium, since our last meeting in Garmisch-Partenkirchen in 2013 a lot of work has been done.

We participated in the plenary session of the European Forum Alpbach (Austria) concerning "Cyberwar — Perceptions and Approaches of Major Actors". There we supported the idea to intensify efforts to improve international law governing international relations in the field of countering military use of ICT.

In April a similar topic was discussed during a meeting on international information security (seminar), held in the Russian Embassy in Stockholm (Sweden) by Russian and Swedish experts. The meeting also addressed the issues of implementation of human rights and freedoms on the Internet.

In late October — early November 2013 in New York (USA) there was a thematic meeting of scientists in the format of the international seminar «Internet governance and management of cyber conflicts: models, regulation and confidence-building measures.» The American side put forward the initiative to make such «synchronization» meetings of scientists and experts an annual event.

MSU experts also participated in the Conference "International cooperation in cyberspace" (Georgetown University, Washington, USA), IV World Summit on Cybersecurity (Stanford, USA), in the Conference "National security and the development of science and technology" (Changsha, China), the first international scientific Conference "Information Security Strategy in the light of strategy Kazakhstan–2050" (Astana, Kazakhstan), and in the Conference "Public-private partnership in the Internet era" (London, UK).

The agenda of our Conference covers important and complex issues of the formation of international information security system, capable of reducing the threat of ICT use for breach of international peace and security.

Firstly, **the issues of adaptation of international law to conflicts in information space.** The discussion at the round table is expected to touch upon the following questions:

- the concept of «Attack» in the information space;
- principles of distinction, proportionality and precautionary measures and their operation in conflicts with the use of ICTs;
- law of neutrality in conflicts with the use of ICTs;
- the concept of «Force» and «Threat of force or Use of force» for information space;
- the concept of «Armed attack» and «Aggression» in information space;

- use of force by means of malicious use of ICT and problems of attribution.

There is a considerable amount of research papers published on almost all of the mentioned issues, but we believe that the desired solution has not yet been found.

This can be partly explained with that the issue at hand is not as much related to gaps or contradictions in the current legislation, but to uncertainty of existing international law interpretations from the standpoint of their applicability to cyberspace, i.e. to the need of adaptation of legal rules to new conditions.

It has been proposed to put the concept of «implicit weapons» at the foundation of the solution of this problem. The substance of this concept lies in the fact that in certain cases the misuse of ICTs gives non-military targets, such as civilian aircraft, nuclear power plants, etc. the properties of «weapons», i.e. tools and mechanisms designed to destroy manpower and equipment. This concept makes it possible to identify sufficiently accurate evidence of the use of ICTs as weapons. And accordingly the conditions when the misuse of ICTs can be recognized as an armed attack, consequently making it possible for victim-state to exercise the inherent right to individual or collective self-defense. It also becomes possible to more accurately determine which norms of international humanitarian law and international law governing the use of force require adaptation to the environment of ICTs misuse.

The second important direction of countering threats to international peace and security in cyberspace is **the information security of critical infrastructures**. This issue will also be discussed in the course of a separate «round table». It is planned to consider the following issues:

- comparative analysis of national approaches to identification of information infrastructure segments as Critical Infrastructure;
- Public-Private Partnership in Critical Infrastructure information security: Best practices, frameworks and recommendations;
- marking and identification of information systems and networks that are protected by international law in cyberspace;
- International System of Monitoring and Objectification of International law violations in relation to Information systems and Networks: Challenges of development.

Some of the mentioned issues have long been a subject of research. 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, on Protection of Victims of International Armed Conflicts, is entirely about the rules of identification. Apparently the application of the Protocol to cyberspace also requires a separate Annex, concerning rules of protected objects identification.

It seems that preparation of objective documentation about facts of international law violations in cyberspace, is still a challenging problem that has no acceptable solution. As we hope, some ideas that could bring together all stakeholders in this field will be expressed in the course of a «round table».

The third important issue to be discussed at the Conference is a **comparative analysis of national approaches and priorities in forming of international information security system**.

The following topics will be discussed in the course of a relevant «round table»:

- legitimization of monitoring and control on networks;
- implementation of national information strategies;
- national cybercrime prevention experience;
- technical surveillance in communication networks in the context of human rights protection;
- international and national approaches to countering the use of the Internet for terrorist and extremist purposes;
- ensuring credibility in cyberspace.

As we see it, each of these issues can become a subject of an independent research in the future. Therefore let's presume that this event will identify their key, 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 of the relevant issues.

Finally, the fourth issue to be discussed at the Conference is technological aspects of international information security, from the standpoint of advanced developments.

With regard to this issue it is proposed to discuss the following issues:

- aggregation, integration and security of Big Data in life sciences and health care;
- implications and impact of emerging biotechnology and nanotechnology on information security;
- application of mathematical sciences to solution of information security issues.

Essentially this «round table» will analyze the factors that determine both present and future perspectives of international information security issues.

Our conference is held as we approach the start of the new UN Group of Governmental Experts on international information security (2014-2015) with the mandate of the UN General Assembly to continue research in this area. It seems that to a certain extent our discussion will be a preparation stage for this event.

In conclusion I would like to mention that over 100 scientists and experts from 21 countries of the world (U.S., Russia, China, Britain, France, Germany, Japan, Australia, Austria, Azerbaijan, Bahrain, Belarus, Bulgaria, Israel, Italy, Kazakhstan, Cambodia, Canada, Kyrgyzstan, UAE, Switzerland), as well as representatives of three international organizations (International Committee of the Red Cross, ICANN (the International Corporation for Assigned Names and Numbers), the European Defence Research and Technology) are participating in our Conference.

Preparation and conduct of such a representative Conference would have been impossible without the help of our sponsors, their representatives are now in the conference hall.

I would like to mention them.

General Director of FSUE "STC" Atlas ", Alexander Gridin;

Scientific Director of Russian Railways Informatics & Automatics Research & Design Institute, Vladimir G. Matyuhin;

ICAAN Vice president, Veni Markovski.

Deep gratitude to all of them.

С.М.Буравлев

Сопредседатель оргкомитета Форума, заместитель Секретаря Совета Безопасности Российской Федерации

Приветствие к организаторам, участникам и гостям Восьмого 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».

В восьмой раз гостеприимный Гармиш-Партенкирхен становится местом встречи специалистов в области информационной безопасности — представителей структур власти, ученых и экспертов научных и образовательных центров ведущих мировых держав. Эта встреча посвящается обсуждению наиболее острых проблем в области информационной безопасности. В современных условиях тематика пленарного заседания, а также вопросов для семинарских дискуссий более чем актуальна.

Стремительное развитие информационно-коммуникационных технологий, их активное внедрение в различные сферы жизнедеятельности государства, общества и личности ставит в число приоритетных задач обеспечение международной информационной безопасности.

Трансграничный характер новых вызовов и угроз безопасности в информационной сфере повышает уязвимость национальных информационных инфраструктур. И, прежде всего, это затрагивает критически важные для национальной безопасности объекты.

Возрастает опасность деструктивных информационных воздействий, представляющих угрозу суверенитету и территориальной неприкосновенности любого государства. При этом отдельная личность, общество в целом также подвергаются негативным информационным воздействиям.

Условия глобализации информационного пространства требуют выбора дальнейшего пути совершенствования международной информационной безопасности. Выбор России, как члена международного сообщества, закреплен в Основах государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. Целеполагающий документ стратегического планирования в этой области утвержден Президентом Российской Федерации 24 июля 2013 года.

В Основах публично заявлена главная цель — содействие установлению международного правового режима, направленного на создание условий для формирования системы международной информационной безопасности.

Достижению этой цели должны способствовать поддержка и активное участие научного, экспертного и бизнес-сообщества.

Форум в Гармиш-Партенкирхене является уникальной площадкой, позволяющей консолидированно обсуждать проблемы в области международной информационной безопасности, совместно выходить на научно выверенные пути решения этих проблем.

При этом важно понимать, что противодействие угрозам безопасности в информационной сфере как на национальном уровне, так и в глобальном масштабе должно носить легитимный характер. Необходимо актуализировать нормы международного права для регламентации деятельности государств в информационном пространстве. Отсюда вытекает неизбежность и настоятельная потребность в исследовании вопросов использования информационно-коммуникационных технологий в межгосударственных конфликтах. Также подлежат исследованию вопросы применимости международного права к сфере использования данных технологий в целом.

Поэтому в повестке дня настоящего Форума приоритет отдан международно-правовым вопросам. Это свидетельство зрелости дискуссионной площадки в Гармиш-Партенкирхене, пример ясного понимания необходимости решения назревших правовых вопросов обеспечения международной информационной безопасности, а также стремления видеть перспективы развития вопросов регулирования отношений в глобальном информационном пространстве.

Полагаю, дискуссии участников Форума приблизят нас к пониманию того, что

- действующие нормы международного права не могут в прямой постановке быть применимы к сфере использования ИКТ;

- эти нормы должны быть усовершенствованы и адаптированы к рассматриваемой области;
- могут и должны быть разработаны новые нормы международного права применительно к сфере использования ИКТ, включая организационно-правовую форму их реализации.

При этом только прикладной характер обсуждения, если позволите, всего периметра «правового поля» использования информационно-коммуникационных технологий будет иметь востребованный результат.

Безусловно, для решения проблем в области обеспечения международной информационной безопасности, формирования на глобальном уровне соответствующей системы необходим не только правовой фундамент, но и базирующийся на этой основе системный подход к решению наиболее острых проблем.

Лавинообразный рост угроз национальной безопасности в информационной сфере диктует необходимость поиска эффективных путей противодействия деструктивным воздействиям на критически важные инфраструктуры. Важно определить как на национальном уровне, так и в глобальном масштабе приоритеты в области формирования системы международной информационной безопасности. При этом системный подход обязывает смотреть на данную проблему сквозь призму перспективных технологических разработок в этой области.

Выражаю надежду, что дискуссионные площадки Форума позволят в полной мере реализовать представленный здесь содержательный интернациональный научный и экспертный потенциал.

Это подтвердит справедливость высокой оценки роли и места Форума, будет способствовать дальнейшему повышению его авторитета, в том числе путем публичного издания полученных результатов.

Желаю организаторам, участникам и гостям 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 organizers, participants and guests of the VIII International Forum «State, Civil Society and Business Partnership on International Information Security»

Dear Colleagues,

Allow me to welcome the organizers, participants and guests of the International Forum «State, Civil Society and Business Partnership on International Information Security».

For the eighth time a welcoming Garmisch-Partenkirchen becomes a meeting place for information security experts — representatives of governments, scientists and experts from scientific and educational centers of the world's leading nations. This gathering is dedicated to discussion of the most pressing issues of information security. In the present context topics of the plenary session and questions for seminar discussions are more than relevant.

The rapid development of information and communication technologies (ICTs) and their active implementation in various areas of state, societal and individual life makes the issue of ensuring international information security a priority.

The transboundary nature of new threats and challenges in the information sphere increases the vulnerability of national information infrastructures. And above all, it affects facilities critical to national security.

Gradually increases the risk of destructive information influences threatening the sovereignty and territorial integrity of any state. At that, individuals and society as a whole are also exposed to negative information influences.

Environment of information space globalization requires a choice of further directions for international information security development. The choice of Russia, as a member of international community, is enshrined in the Principles of State Policy of the Russian Federation in the field of international information security for the period until 2020. Purposeful document of strategic planning in this area was approved by the President of the Russian Federation on July 24, 2013.

The Principles publicly state the main objective — to promote an international legal regime aimed at creating the conditions for the formation of an international information security system.

Support and active participation of scientific, expert and business community should contribute to achievement of this objective.

Forum in Garmisch-Partenkirchen is a unique platform that allows a consolidated discussion of international information security problems and together develop scientifically verified paths to solutions to these problems.

It is important to understand that countering security threats in the information sphere both nationally and globally should be legitimate. It is necessary to update the norms of international law to regulate the activities of nation-states in information space. Hence the inevitable and urgent need to research the use of ICTs in international conflicts. The issue of general applicability of international law to the use of these technologies should also be investigated.

Therefore, the agenda of the Forum gives priority to international legal issues. It indicates the maturity of this discussion platform in Garmisch-Partenkirchen. It is an example of clear understanding of the need to solve the urgent legal issues of international information security, and aspiration to see the development prospects of the global information space relations regulation.

I believe the discussions in the course of the Forum will bring us closer to understanding that

the existing rules of international law cannot be directly applied to the sphere of ICTs use;

these rules should be improved and adapted to this sphere;

new rules of international law concerning the sphere of ICTs use can and should be developed, including procedural and institutional form of their implementation.

However, only applied nature of the discussion of, so to speak, entire «legal field» of ICTs use will yield the required result.

Needless to say, the solution of international information security issues and formation of the corresponding global system requires not only legal foundation, but also a hereon based systematic approach to solving the most pressing problems.

A surge of national security threats in the information sphere necessitates the search of effective ways to counter destructive effects on critical infrastructure. Both nationally and globally it is important to identify priorities of international information security system formation. And systematic approach requires looking at the problem in the light of perspective technological developments in this area.

I hope that the Forum discussions will fully unlock the extensive international scientific potential and expertise represented here.

This will confirm that high appreciation of the role and place of the Forum is just and fair, and will further enhance its authority, among other things through open publication of the proceedings.

I wish the organizers, participants and guests successful and fruitful work!

Чарльз Барри[1]

Центр технологий и политики национальной безопасности
Национальный университет обороны, США

Вызовы защиты критически важной инфраструктуры: Надежность систем в цифровой век

1. Введение

Благодарю Вас, д-р Шерстюк, а также спонсоров и организаторов за приглашение принять участие в Форуме по информационной безопасности. Идиллическая картина альпийской весны, которую мы можем наблюдать в Гармише, приглашает всех нас на несколько дней оставить в стороне озабоченность мировыми проблемами и приложить усилия к обеспечению безопасности киберпространства ради нашего общего будущего.

Сегодня утром меня попросили выступить с докладом о проблемах защиты критической инфраструктуры. Этот вопрос имеет глобальное значение и, таким образом, является достойным предметом обсуждения для такой международной группы экспертов, как та, что собралась здесь сегодня. Существует множество физических и кибер-рисков, от которых необходимо защищать критически важную инфраструктуру — от механических повреждений в результате стихийных бедствий до простых человеческих ошибок, и, конечно, злоумышленных действий, совершаемых преступниками или организациями. Защита должна быть устойчивой, надежной и долговечной — как в мирное время, так и во время кризиса или конфликта.

Сегодня давайте обратим внимание на защиту критически важной инфраструктуры от рисков, исходящих из киберпространства, или, если хотите, рисков в информационной сфере. Мы также можем рассмотреть и риски физических угроз, которые являются не менее серьезными, однако тематикой нашего Форума является информационная безопасность. Приступим.

---

[1] Отказ от ответственности: в настоящей статье изложена личная точка зрения Чарльза Барри, которая не обязательно отражает политику Национального университета обороны, Министерства обороны или Правительства США.

2. Критически важная инфраструктура

Итак, что именно представляет собой критически важная инфраструктура? Как представляется, она многочисленна. Рассмотрим пару перефразированных определений — одно национальное и одно региональное:

- В США критически важная инфраструктура определяется как «системы и средства, которые настолько жизненно важны для США, что их неработоспособность или уничтожение оказали бы угнетающее воздействие на национальную безопасность, экономическую безопасность, здравоохранение и правопорядок».
- В Европейском союзе используется подобное определение. «Критически важная инфраструктура Европейского союза — это средства или системы, необходимые для поддержания работы жизненно важных общественных функций, таких как здравоохранение, безопасность, правопорядок и экономическое благополучие; их выведение из строя или разрушение окажет значительное влияние на государства-члены ЕС».

Что касается критически важной инфраструктуры США, Министерство национальной безопасности США выделяет 16 различных секторов критически важной инфраструктуры, в том числе: банковский сектор; химическая промышленность; связь; критически важные производства; плотины; оборонно-промышленный комплекс; образовательные учреждения; аварийные службы; энергетический сектор; сектор продовольствия и сельского хозяйства; государственные учреждения; общественное здравоохранение; информационные технологии; сектор ядерной промышленности; национальные памятники; водоснабжение.

Важно принять во внимание, что определение, что является критически важным, часто зависит от того, какое агентство вы об этом спрашиваете. В небольшом городке с единственным колодцем, или единственным мостом, или единственной телефонной линией, или единственной дорогой — все эти элементы инфраструктуры города, разумеется, считаются «жизненно важными», и их потеря окажет «разрушительное» воздействие на горожан и их выборных должностных лиц. Однако для государства нереалистично обозначить каждую небольшую дорогу, мост, телекоммуникационную сеть или источник воды, как национальную критически важную инфраструктуру, даже если политически оно иногда должно рассматривать их как таковую. Было бы невозможно вкладывать средства в защиту *всех* инфраструктур, зависящих от

киберпространства. Более того, если всё считать критически важным, то ничто таковым не будет. Не будет приоритетов, согласно которым распределяются ресурсы. Таким образом, ответ «всё» не лучше, чем ответ «ничего». Необходимо принять ряд трудных решений, и даже среди них необходимо выделить приоритеты.

Вообще, значительная часть международной литературы по критически важной инфраструктуре содержит аналогичные списки важнейших секторов инфраструктуры, подобные вышеупомянутым. Однако необязательно иметь согласованный на международном уровне список того, что является критически важной инфраструктурой, а что нет. Скорее всего, на международном уровне будет нелегко договориться об общепринятом определении, и в любом случае такой «список» необходимо будет постоянно обновлять. Он будет бесполезным. Тем не менее, некоторая взаимная транспарентность была бы полезна — в отношении того, что каждая нация считает своей критически важной инфраструктурой. Речь идёт главным образом об указании категорий, но, возможно, также об указании ряда основных объектов и систем общего пользования.

Конечно, кроме двух вышеприведённых, существуют и другие национальные и международные определения, но и по этим определениям можно легко понять, что защита критической инфраструктуры будет непростой задачей, и, несомненно, всегда будут присутствовать элементы риска. В каждом государстве есть множество критически важных инфраструктур, есть также международные критически важные инфраструктуры, в первую очередь система подводных волоконно-оптических кабелей, которая в основном принадлежит транснациональным корпорациям, но в значительной степени находится в международных водах.

С какими угрозами мы сталкиваемся сегодня и в будущем, пытаясь обеспечить безопасность этих критически важных систем? Что должно вызывать беспокойство?

3. Угрозы критически важной инфраструктуры

Продолжая рассмотрение американской модели, США при обеспечении безопасности инфраструктуры, для охвата как физического, так и киберпространства, используют «всеобъемлющий подход к защите инфраструктуры». Недавно стало понятно, что это абсолютно правильный подход. Когда в 2012 году ураган Сэнди обрушился на район Карибского моря,

восточную часть США и Канады, угроза критически важной инфраструктуре проявилась в виде крупномасштабного физического уничтожения, вызванного природой — штормовым ветром, грозами и сильным наводнением. В результате урагана Сэнди 10 миллионов человек на восточном побережье США остались без электричества, некоторые из них находились в таком состоянии на протяжении многих недель, без тепла, воды или электричества. И это несмотря предпринятые на всех уровнях власти (федеральном, местном и на уровне штатов) меры по предупреждению и ликвидации аварий в виде множества электроремонтных бригад со всей территории Соединенных Штатов и Канады. За 48 часов было отменено более 5000 коммерческих рейсов авиакомпаний. Из-за наводнения были закрыты станции метро в центре Нью-Йорка и Вашингтона. Беспрецедентно на два дня прекратила работу Нью-Йоркская фондовая биржа. Погибло 285 человек. Общие потери составили более $ 10 млрд. Значительная часть критически важной инфраструктуры была разрушена.

Но является ли защита критически важной инфраструктуры от угроз, исходящих из киберпространства, на самом деле настолько же, или даже более важной, чем защита от угрозы физического ущерба от естественных причин? Центр стратегических и международных исследований и компания компьютерной безопасности McAfee, в своём исследовании 2013 года, пришли к выводу, что ежегодные потери от киберпреступлений, затрагивающих критически важную инфраструктуру, в США составляют $ 100 млрд. Эта оценка является радикальным пересмотром и составляет 1/10 от предыдущей оценки McAfee в $ 1 трлн ежегодных потерь. Таким образом, по материалам Wall Street Journal, ежегодные потери от киберпреступности, целью которой часто становится сектор финансовых услуг, находятся на одном уровне с ежегодным ущербом от происшествий на автотранспорте. Однако в исследовании ЦСМИ и McAfee не были учтены такие долгосрочные потери, как утрата конкурентоспособности из-за кражи информации, составляющей коммерческую тайну.

Давайте не будем обманывать себя: исходящие из киберпространства риски для критически важной инфраструктуры являются реальными и возрастают по мере того, как неуклонно увеличивается и становится всё более необратимой наша зависимость от этих систем. Для того, чтобы подчеркнуть всю серьёзность рисков, приведём несколько громких дел.

Произошедшие в конце 2012 года кибератаки типа распределенный отказ в обслуживании (DDoS) на американские банки стали для США тревожным сигналом. После этих атак в июле 2013 года были проведены учения под названием «Квантовый рассвет — 2», в которых приняли участие более 50 банков, а также Комиссия по ценным бумагам и биржам, ФБР, Министерство финансов и Министерство внутренней безопасности США. Существует реальная вероятность, что с увеличением количества совершаемых пользователями транзакций в Интернете, возрастёт число онлайн-атак.

Кроме DDOS-атак, угрозу нашей инфраструктуре представляют: преступники, которые хотят украсть деньги; «Хактивисты», которые посредством нарушения работы критически важных систем хотят сделать политические заявления; а также иностранные правительства, целью которых является шпионаж, направленный против транснациональных компаний США и других государств.

Кроме этого, из последних примеров можно привести вирус Shamoon, который в 2012 году поразил ключевые компании энергетической инфраструктуры (нефти и природного газа) на Ближнем Востоке — Saudi Arramco (Саудовская Аравия) и Ras Gas (Катар). Как утверждается, эти нападения были осуществлены каким-то государством или от его имени.

Еще одним широко освещённым примером нападения на инфраструктуру является атака вируса Stuxnet на программируемые логические контроллеры (ПЛК) на территории комплекса по обогащению урана в иранской Натанзе. Считается, что эта атака является первым примером использования специализированного кибероружия, хотя для подтверждения этого необходимо гораздо больше информации и исследований.

Другой важной и растущей проблемой являются продвинутые постоянные угрозы (Advanced Persistent Threat). Они являются хорошо организованными, направлены, как правило, на цели, имеющие наибольшее значение, в том числе системы инфраструктуры, и их вредоносный код трудно обнаружить и устранить внутри сети. Эти угрозы зачастую не оставляют обнаружимых следов своего присутствия, они просто находятся внутри сети и либо извлекают данные, наблюдают за сетевой активностью, или внедряют вредоносные программы для последующего использования, в том числе для выведения сети из строя в решающий момент.

Мы стали свидетелями политически мотивированных атак на государства, например, нападений на эстонские банков-

ские, информационные и правительственные веб-сайты весной 2007 года. В этом случае, несмотря на то, что некоторые считали его нападением на эстонское государство, было установлено, что это были «кибербеспорядки», осуществленные «хактивистами». Они действовали самостоятельно или в качестве прокси в ответ на неприемлемое для русских решение правительства Эстонии по перемещению памятника с центральной площади Таллинна.

И, естественно, будут иметь место такие нападения на инфраструктуру в рамках кинетических межгосударственных конфликтов как, например, атаки на грузинские системы во время российско-грузинской войны 2008 года. Еще только предстоит определить, как эти атаки могут нарушать законы вооруженных конфликтов с точки зрения их потенциала непропорциональных гражданских потерь или неизбирательного уничтожения. Во второй половине дня на эту тему будет более обширный доклад д-ра Санджая Гоэла.

Похожими, но, в связи с отсутствием обычной военной кампании, другими были кибератаки против информационных систем Украины и НАТО во время недавней российской подрывной деятельности и аннексии Крымской области Украины. Несомненно, можно сделать вывод, что любая будущая деятельность по всему спектру военных операций будет включать в себя киберкомпонент.

Таким образом, выше перечислен спектр возрастающих угроз, и этот короткий список без сомнения является неполным. Единственное, что мы можем сказать с практически полной уверенностью: угрозы никуда не уходят, а становятся все более распространенным явлением и всё более изощренными. Далее мы обратим внимание на то, что государства и международные организации делают для противодействия этим угрозам.

4. Основные элементы системы защиты критически важной инфраструктуры США.

За каждым из шестнадцати секторов критической инфраструктуры США был закреплён соответствующий орган федеральной власти. Большинство секторов находятся в ведении Министерства внутренней безопасности. Некоторые сектора работают с другими ведомствами, например, оборонно-промышленный сектор с Министерством обороны, а банковский сектор с Министерством финансов.

В каждом секторе есть соответствующий Центр обмена информацией и анализа, в ведении которого находится государственно-частное партнерство и добровольный обмен информацией об угрозах и методах защиты. Этот обмен очень важен, поскольку примерно 85% критически важной инфраструктуры США находится в частном секторе, а стороны, участвующие в этих партнерствах от государства, как правило, лучше осведомлены об общих угрозах, чем любая частная корпорация или предпринимательский сектор.

Для каждого выделенного сектора был разработан Национальный план по защите инфраструктуры и ряд Специальных секторальных планов. Они разработаны с учетом Национальной программы по чрезвычайным ситуациям, которая является всеобщим планом США по реагированию на различные бедствия и чрезвычайные ситуации, не только в киберпространстве.

В феврале 2014 года президент Обама представил первые добровольные стандарты кибербезопасности, чтобы бизнес использовал их при защите своей критически важной инфраструктуры. Стандарты также поощряют более широкий обмен информацией между секторами бизнеса и соответствующими государственными органами. Это первый шаг. Трудно и потенциально экономически вредно заставлять конкурирующие компании обмениваться информацией об успешных нападениях на них. Тем не менее, следование стандартам со временем должно стать нормой. В конце концов, возможно, также появится закон, предписывающий соблюдать эти требования.

В рамках своих обязанностей по оказанию помощи оборонно-промышленному сектору Министерство обороны выдвинуло Расширенную инициативу по кибербезопасности. Её целью является обмен информацией об угрозах и защите с оборонными подрядчиками, являющимися частью критически важной инфраструктуры. Аналогичные инициативы для оказания помощи другим секторам в настоящее время разрабатываются другими ведомствами, в первую очередь Министерством национальной безопасности.

Наконец, Международная стратегия для киберпространства США направлена на «предоставление государствам, стремящимся создать свой собственный технический потенциал и потенциал кибербезопасности, необходимого опыта, знаний и других ресурсов». Поддержка США ранжируется от поддержки национального потенциала в области ликвидации

последствий инцидентов до создания государственно-частных партнерств, повышения безопасности систем управления, помощи в создании эффективных законов по киберпреступности. США работают с другими странами как самостоятельно, так и в рамках форумов под эгидой ОАГ, АТЭС, НАТО и ООН.

5. Краткий обзор деятельности международных организаций по защите инфраструктуры

Организация Объединенных Наций

С 2004 года растёт доверие к работе Группы правительственных экспертов ООН (ГПЭ), как одной из наиболее многообещающих инициатив по международному сотрудничеству. Достигнутые в 2010 и 2012 годах в рамках ГПЭ договоренности были скромными, но примечательными — как обычно и бывает в начале такой работы. Каждый из докладов был более содержательным, чем предшествующее (принятию доклада в 2010 году предшествовала неудача), и мы должны с оптимизмом надеяться, что очередной раунд переговоров продолжит эту тенденцию, несмотря на то, что он будет проводиться среди более широкой группы экспертов. Говорить что-либо о положительной динамике ГПЭ более не стоит, потому что нам повезло, и со следующим пленарным докладом будет выступать посол Андрей Крутских. Он хорошо известен всем нам как один из первоначальных членов ГПЭ, председатель ГПЭ 2010 года, и закаленный ветеран, который этим летом будет снова участвовать в переговорах во время очередного раунда дискуссий. Без сомнения, Андрей сообщит нам некоторые ценные сведения, о том, что ожидать на протяжении очередных двух лет работы ГПЭ, и что ожидать в будущем. Важно четко понимать, что ООН активно участвует в развитии международной кибербезопасности.

Международный союз электросвязи

МСЭ представил проект Глобальной программы кибербезопасности в 2007 году, который основывается на пяти столпах, это: нормативно-правовая база; технические меры; организационные структуры; наращивание потенциала; и международное сотрудничество. МСЭ является ведущей глобальной действующей силой по мерам укрепления доверия в секторе ИКТ. Одним из его наиболее заметных проектов

является Индекс глобальной кибербезопасности, в котором даётся оценка возможностей кибербезопасности государств по пяти критериям: правовые, технические и организационные меры, наращивание потенциала и сотрудничество. МСЭ поддерживает партнерские отношения с другими организациями: с Управлением ООН по наркотикам и преступлениям для обмена передовым опытом по нормотворческой деятельности в области киберпреступлений; с Международным многосторонним партнерством против киберугроз, для работы над глобальными решениями проблем противодействия киберугрозам; и с Форумом групп обеспечения безопасности и реагирования на инциденты для обмена передовым опытом о возможностях реагирования на компьютерные инциденты.

Европейский союз

В вопросе международной кибербезопасности, ЕС является, пожалуй, наиболее активной региональной организацией, что является следствием крепких бюрократических основ. В 2004 году в ЕС было создано Европейское агентство сетевой и информационной безопасности с центральным офисом на Крите — в этом году агентство отмечает свое 10-летие. Также с 2004 года в ЕС начали заниматься вопросами защиты инфраструктуры, а в 2009 году для развития обмена информацией было создано Государственно-частное партнерство для повышения устойчивости. В начале прошлого года была принята Стратегия кибербезопасности ЕС, а в августе 2013 года обновлена Европейская программа защиты критически важной инфраструктуры, и выделено три направления работы: предупреждение, повышение готовности и реагирование.

В Европейской программе защиты критически важной инфраструктуры выделено четыре приоритетных общеевропейских сектора: система организации воздушного движения Евроконтроль; глобальная навигационная спутниковая система Galileo; Сеть электропередач и Европейская газотранспортная сеть.

В ЕС разработана Информационная сеть предупреждения критически важных инфраструктур — основанная на Интернете, эта система предназначена для обмена идеями по защите критически важной инфраструктуры, исследованиями и передовым опытом между странами-членами ЕС и их учреждениями. Портал Информационной сети начал работу в середине января 2013 года. В соответствии с программой Циф-

ровой повестки дня для ЕС, под руководством Европейского агентства сетевой и информационной безопасности, были дважды проведены общеевропейские учения по кибербезопасности, в ходе которых были проверены системы обеспечения безопасности критически важной инфраструктуры на всей территории Европейского союза. Также были определены минимальные базовые возможности, услуги и политические рекомендации, необходимые для эффективного функционирования национальных/государственных Групп быстрого реагирования на компьютерные инциденты.

Организация Североатлантического договора (*НАТО*)

НАТО принимает участие в защите критически важной инфраструктуры с 2001 года. В 2003 году Главный комитет по планированию использования гражданских служб в чрезвычайных ситуациях принял план из шести пунктов для помощи государствам в ликвидации последствий химических, биологических, радиологических и ядерных атак, особенно террористического характера. В 2006 году главы государств и правительств подтвердили роль Альянса по защите критически важной инфраструктуры для защиты населения, территории, инфраструктуры и вооруженных сил стран-участниц от последствий террористических атак, а также для защиты собственных интересов безопасности от прерывания потока жизненно важных ресурсов.

В 2011 году в рамках Альянса началась работа по выявлению зависимостей критически важной инфраструктуры стран-участниц и работа с ними по оценке уязвимости систем, жизненно важных для миссий и операций Альянса. Как ожидается, в 2014 году министры Альянса утвердит новую политику кибероборонь, которая за несколько ближайших лет поспособствует укреплению программ НАТО.

Совсем недавно, 5-8 апреля, Североатлантический совет принял решение удовлетворить просьбу Украины, страны-партнера НАТО. Для оказания помощи Украине в разработке гражданских планов действий в чрезвычайных ситуациях и антикризисных мер была направлена Консультативная группа поддержки НАТО по защите критически важной инфраструктуры и гражданского населения. Это связано с критически важной энергетической инфраструктурой и угрозами безопасности жизнедеятельности в случае дальнейшего ухудшения там условий безопасности.

Организация по безопасности и сотрудничеству в Европе (*ОБСЕ*)

ОБСЕ проявила всеобщий интерес к кибербезопасности, как транснациональной проблеме, на саммите в 2010 году, а также на специальной конференции по кибербезопасности в 2011 году. В декабре 2013 года в ОБСЕ было согласовано «Решение о первоначальном перечне мер укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий». В этот перечень входит, кроме прочего, добровольное проведение консультаций на соответствующем уровне для снижения риска неправильного восприятия... и защиты критически важной национальной и международной инфраструктуры ИКТ, в том числе обеспечения их целостности.

Организация исламского сотрудничества

Организация исламского сотрудничества является еще одной региональной организацией, которая предпринимает шаги для решения проблемы защиты критически важной инфраструктуры, однако путём консультирования заинтересованных стран-участниц для укрепления их потенциала на национальном уровне. В 2008 году была создана Группа экстренного реагирования на компьютерные происшествия Организации исламского сотрудничества, и на сегодняшний день в неё вошли соответствующие группы 19 из 57 стран-участниц. Ежегодно ими проводится 2-5 конференций для обмена передовым опытом, нормами и сведениями об угрозах. Только некоторые из этих обсуждений посвящены защите критически важной инфраструктуры, но это хорошее начало. Необходимо всемерно приветствовать даже небольшие шаги и способствовать развитию их содержательности и прозрачности. И все большему количеству стран-участниц Организации исламского сотрудничеств следует принимать в этом участие. Это особенно важно для Афганистана, который стремится обеспечить надежность ИКТ-инфраструктуры для поддержания экономики, пытающейся встать на предпринимательские рельсы по мере ухода Международных сил содействия безопасности к концу этого года.

Африканский союз

В январе 2012 года Африканский союз разработал проект Конвенции по доверию и безопасности в киберпространстве.

Заявленной целью Конвенции является создание надежной основы для кибербезопасности в Африке. Это первый обнадеживающий шаг к участию Африканского союза в защите критически важной инфраструктуры. Конвенция должна была быть принята в январе 2014 года, но это не было сделано из-за возражений Кении по вопросу конфиденциальности. На следующем этапе Кения представит свои письменные возражения к маю 2014 года.

Организация американских государств (*ОАГ*)

В 2004 году члены ОАГ одобрили резолюцию, в соответствии с которой Секретариат начал работу над вопросами кибербезопасности. Целью этой работы стало создание Групп экстренного реагирования на компьютерные происшествия в каждом государстве-члене, и Группы экстренного реагирования на компьютерные происшествия ОАГ, как механизма координации региональных инициатив в области кибербезопасности. Согласно последним данным, большинство членов ОАГ в 2011 году имели Группы экстренного реагирования на компьютерные происшествия. Это свидетельствует, что программа в значительной степени была успешной. Пока неясно, насколько активно Группа экстренного реагирования на компьютерные происшествия ОАГ консультирует членов организации или организует перспективные программы помощи, подобные программам Организации исламского сотрудничества.

Ассоциация государств Юго-Восточной Азии (*АСЕАН*)

В Сингапурской декларации 2003 года содержался призыв к созданию информационной инфраструктуры АСЕАН и Групп экстренного реагирования на компьютерные происшествия во всех государствах-членах к 2005 году. В 2010 году был принят Генеральный план развития связи в странах АСЕАН. В 2011 году был согласован Генеральный план развития ИКТ в АСЕАН до 2015 года. В 2012 году, для оказания поддержки Совету АСЕАН по сетевой безопасности, странами АСЕАН было принято решение о продолжении учений, проводимых Группой экстренного реагирования на компьютерные происшествия АСЕАН. В 2013 году была обновлена программа сотрудничества по сетевой безопасности 2005 года.

Азиатско-Тихоокеанское экономическое сотрудничество (*АТЭС*)

Начиная с 2002 года, АТЭС принял ряд документов по кибербезопасности, в том числе Стратегию кибербезопасности 2005 года, в которой была признана важность безопасности инфраструктуры связи, и, в частности, Интернета в регионе АТЭС.

Шанхайская организация сотрудничества (*ШОС*)

В марте 2013 года странами ШОС были подписаны соглашения по борьбе с использованием или потенциальным использованием компьютерных сетей в террористических, сепаратистских или экстремистских целях. Хотя эти соглашения, как представляется, не предназначены для совместного решения проблем защиты критически важной инфраструктуры, они, тем не менее, свидетельствуют о текущей деятельности ШОС в этой области.

Без сомнения, во всём мире существуют и другие инициативы, и присутствующие здесь в зале могут дополнить этот список в ходе обсуждения. Вышеприведенные примеры демонстрируют, в какой степени ООН и многие региональные организации начинают решать неизменную задачу защиты критически важной инфраструктуры. Есть ли среди них такие, которые делают всё от них зависящее? Полагаю, все согласятся, что они могут и должны делать больше. А все, что они уже делают, должно осуществляться более эффективно, и в соответствии с более высокими стандартами, к которым они сами стремятся. Необходимо взаимодействовать с ними, и способствовать тому, чтобы движение вперёд было энергичным, транспарентным и совместным.

6. Заключение

Этот краткий обзор критически важной инфраструктуры и некоторых действующих инициатив по её защите должен стимулировать обсуждение, а в идеале, и новое мышление о том, как бороться с соответствующими проблемами на международном уровне.

Позвольте мне предложить для такого обсуждения три направления работы, которые, как представляется, являются первостепенными. Прежде всего, мы должны работать над повышением устойчивости наших критически важных систем, как новых, так и старых, и вкладывать средства в улучшение систем по мере возникновения рисков, или упреждая

ожидаемые. Мы должны работать над этим на национальном уровне через государственно-частное партнерство, а также на региональном и глобальном уровнях.

Мы также должны вкладывать средства в противодействие организации и распространению ботнетов, в том числе сетей, арендуемых для криминальных целей. Это потребует от государств принятия на себя ответственности по недопущению противоправного поведения на их территории. Для этого также потребуется повысить скорость и качество сетевой судебной экспертизы, и найти способы осуществлять фильтрацию интернет-трафика, скорее всего, на уровне Интернет-провайдеров. Есть множество веских причин, почему фильтрация не получила широкого распространения — задержки, затраты, конфиденциальность, и т.д. Нам необходимо найти такие решения, которые бы удовлетворили различных участников, в том числе Интернет-провайдеров и самих пользователей.

Что касается компьютерной экспертизы, предмет которой шире, чем вышеприведенный пример, а также политики фильтрации, нам нужны гораздо более образованные и осведомленные трудовые ресурсы — которые в совокупности намного лучше разбираются в передовой практике и компьютерной гигиене. Это человеческое измерение защиты критически важной инфраструктуры слишком часто упускается из виду. Не это приносит прибыль технологическим компаниям, продающим решения сетевой безопасности. Однако, мало кто сомневается, что это самое слабое место в системе обеспечения безопасности. Честные и имеющие соответствующий допуск пользователи неосознанно просто сами допускают хищение данных своих учетных записей — по причине использования плохих паролей, посторонних устройств в сетях, непроверенных механизмов аутентификации, или будучи жертвами целевого фишинг-мошенничества. Будет ли следующее поколение пользователей, выросшее в сети, лучше разбираться в вопросах безопасности? Возможно, но это неочевидно, принимая во внимание ту лёгкость, с которой личная информация размещается в социальных сетях. Необходимо внедрить компьютерную безопасность в каждый метод и образовательную дисциплину. Конечно, технология может в этом помочь, если безопасность будет встроена по умолчанию.

Активная оборона и разведка внутри критически важных информационных сетей является еще одним важным элементом защиты. Сетевые администраторы должны иметь воз-

можность обнаружения вредоносных программ не только на граничных порталах, но также и в пределах своих сетей для обнаружения скрывающихся в них несанкционированных агентов, маскирующихся под зарегистрированных пользователей.

Как было отмечено в начале этого доклада, мы также не можем игнорировать физическую угрозу в отношении информационных систем, будь то стихийное бедствие, как ураган Сэнди, террористический акт или какая-либо другая разрушительная сила. Так же, как и меры защиты киберпространства, меры физической защиты должны включать в себя повышение надёжности, резервирование и необходимые барьеры, а также динамическую защиту, например активные системы наблюдения — автоматизированные или управляемые оператором.

Чтобы со временем защита стала и оставалась адекватной, нам нужно расставить приоритеты и вложить достаточные ресурсы. Мы должны решать проблемы на двух направлениях — на уровне конечных пользователей, посредством таких образовательных программ, как Stop-Think-Connect; а также посредством усиления защиты ключевых узлов инфраструктуры, где мы можем одновременно оградить от угроз миллионы систем и IP-адресов. Мы должны активно работать и на том, и на другом направлении, а не просто вкладывать средства в одно из них.

Наконец, для своевременного восстановления систем и ограничения последствий отказа инфраструктуры, необходимо совместное реагирование, которое потребует от нас соответствующих возможностей, взаимодействия и развития устойчивости. Когда у нас будут все эти возможности, мы будем двигаться в нужном направлении и будем хорошо подготовлены для решения существующих и будущих проблем защиты критически важной инфраструктуры.

Dr. Charles (Chuck) Barry[1]

Center for Technology & National Security Policy
National Defense University, Washington, D.C., the USA

Challenges in the Protection of Critical Infrastructure Systems Reliability in the Digital Age

1. Introduction

Thank you Dr. Sherstuyk and thanks as well as to the many sponsors and organizers for inviting me to participate at this year's Forum on Information Security. The idyllic alpine setting of springtime here in Garmisch invites us all to leave aside the concerns of the broader world for a few days and invest our energies in the business of securing cyber space for our common future.

This morning I've been asked to address the challenges of protecting critical infrastructure, an issue of global importance and thus a fitting subject of discussion by an expert international group such as is convened here today. The physical and cyber risks from which critical infrastructure must be protected are many, from mechanical failure to natural disasters to simple human error and, yes, malicious acts, either by criminals or organizations. Protection must be resilient, reliable and enduring whether during times of peace, crisis or conflict.

Today let us concentrate on the protection of critical infrastructure from risks emanating in cyber space, or if you like, risks within the information realm. We can touch on physical threats too, which are no less serious but the nature of our Forum is information security. Let us begin.

2. Critical Infrastructure

So, what is critical infrastructure exactly? It would seem we have a lot of it. Here are a couple of paraphrased definitions to consider, one national and one regional:

- The U.S. defines *Critical Infrastructure* as 'those systems and assets so vital to the United States that their incapacity or destruc-

[1] Disclaimer: The view's expressed in this paper are Dr. Barry's alone and do not necessarily reflect the policies of the National Defense University, the Department of Defense or the United States Government.

tion would have debilitating impact on national security, economic security, public health or safety.

- The EU uses a very similar definition by saying *European Union Critical infrastructure* is assets or systems essential for the maintenance of vital societal functions such as health, safety, security, and economic well-being whose disruption or destruction would have a significant impact in a Member State.

For U.S. critical infrastructure, the federal Department of Homeland Security goes on to list 16 distinct sectors of critical infrastructure including: banking; chemical; communications; critical manufacturing; dams; defense industries; education facilities; emergency services; energy sector; food and agriculture; government facilities; public health; information technologies; nuclear sector; national monuments; and water.

One observation we should keep in mind is that what is critical often depends on what agency is being asked. In a small town with but one water well or one bridge or one telephone line or one road, certainly all these elements of the town's infrastructure are considered "vital," and their loss would be "debilitating" to the townspeople and their elected officials. But it is unrealistic for a nation to define every small road, bridge, telecommunications link or water source as critical infrastructure on a national scale, even if politically it must at times regard them as such. It would be impossible to invest in the protection of *all* infrastructures that depends on cyberspace. Moreover, if everything is considered critical, nothing will be. There would be no priorities on which to allocate resources. So, 'everything' is no more an answer than 'nothing.' Tough choices are needed, and even within them, priorities will have to be set.

In fact much of the international literature on critical infrastructure offers similar lists of critical infrastructure sectors such as those cited above. However, it is not necessary to have an internationally agreed list of what is critical and is not critical infrastructure. We would likely find it hard to agree among many nations on a common definition, and in any case, such a 'list' would need continuous updating. Its utility would be meaningless. Nonetheless, it would be helpful to have a degree of mutual and reciprocal transparency with respect to what each nation regards as its critical infrastructure, mainly by category but perhaps also by noting a number of major public installations and systems.

There are surely other national and international definitions besides the two given above, but from these definitions we can

readily see that protecting critical infrastructure will be a daunting task, and there will undoubtedly always be elements of risk. There is a lot of critical infrastructure in all of our nations, and there are international critical infrastructures as well, most notably the system of undersea fiber optic cables mainly owned by multinational corporations but largely located in international waters.

If these are the critical systems we are trying to protect, what are the threats that we face today and into the future? What should we be worried about?

3. Threats to critical infrastructure

Keeping with the American model, the U.S. takes an 'All-Hazards Approach to Infrastructure Protection' in order to address the physical as well as the cyber dimension. Recently, this proved to be exactly the right approach. When Hurricane Sandy struck the Caribbean, the eastern U.S., and Canada in 2012 the threats to critical infrastructure came in the form of massive physical destruction caused by nature — high winds, violent electrical storms and massive flooding. Hurricane Sandy took 10 million people off the electric power grid along the U.S. East coast, some of them for many weeks, leaving them without heat, water or power, this in spite of federal, state and local emergency responses that brought legions of power line repair crews in from all across the United States and Canada. More than 5,000 commercial airline flights were canceled in one 48 hour period. The central New York and Washington subways systems were closed due to flooding. The New Your Stock Exchange had two unprecedented days of closure. 285 people lost their lives. More than $10 Billion in damage overall. Much critical infrastructure was destroyed.

But with regard to threats from cyber space, is protecting critical infrastructure really as important or more so that the threat of physical damage from natural causes? A summer 2013 study by the think tank Center for Strategic and International Studies and the computer security firm McAfee concluded the annual cost of cybercrime involving critical infrastructure in the U.S. was an estimated $100 billion. That estimate was a sharp downward revision to only one-tenth of what McAfee had reported before for the same period — an earlier estimate of $1 trillion in annual losses. That put annual cybercrime losses, often directed at the financial services sector, on a par with the annual cost of automobile accidents according to the Wall Street Journal. However the longer term costs, such as lost competitiveness due to the theft of proprietary

commercial information, were not factored in to the CSIS-McAfee revisions.

So let's not kid ourselves: the risks to critical infrastructure from cyber space are real and expanding even as our dependence on these systems grows inexorably greater and more irreversible. Several high profile cases underscore the grave risks we all face.

Cyber attacks in the form of Distributed Denial of Service (DDOS) attacks on American banks in late 2012 were a particular wake-up call in the US. These attacks led to the industry-wide exercise Quantum Dawn 2 in July 2013, where more than 50 banks, plus the Security and Exchange Commission, FBI and Departments of Treasury and Homeland Security participated. There is the distinct possibility online attacks will grow as customers do more transactions online.

Besides DDOS attacks, threats to our infrastructure include: Criminals who want to steal money; Hacktivists" who want to make political statements by disrupting critical system; and foreign governments that want to spy on American and other nation's multinational companies.

In addition, we have the recent example of the 2012 Shamoon virus attacks on Saudi Arramco (Saudi Arabia) and Ras Gas (Qatar), key companies in the Middle East energy (petroleum and natural gas) infrastructure. These attacks were alleged to have been conducted by or on behalf of a nation state.

Another recent, amply reported infrastructure attack was the Stuxnet attack on programmable logic controllers (PLCs) within the uranium enrichment complex at Natanz, Iran. This attack is considered by some as the first use of a specific cyber weapon, although much more information and analysis is needed before that claim can be confirmed.

Advanced Persistent Threats are another growing and high profile concern. APTs are sophisticated, tend to go after high value targets including infrastructure systems, and their malicious code is hard to detect and eliminate inside a network. APTs often have no detectible presence, they simply reside inside a network and either exfiltrate data, report on network activity, or plant malware for later exploitation, including taking down the network at a critical time.

We have seen politically motivated attacks against nation states such as the attacks on the Estonian banking, information and government websites in spring 2007. In that case, although some regarded it as an attack against the state of Estonia, it was determined to be a 'cyber riot' by hactivist, acting on their own or as proxies,

in response to an Estonian decision, unpopular with Russians, to relocate a monument from the capital's (Tallinn) central square.

It should come as no surprise that there will be infrastructure attacks as part of kinetic inter-state conflicts, such as the Georgian systems attacked during the Russo-Georgian war of 2008. What is yet to be defined is how these attacks might transgress the Laws of Armed Conflict in terms of their potential for disproportionate civilian casualties or indiscriminate destruction. We will hear much more on this topic from Dr. Sanjay Goel this afternoon.

Similar, yet not exactly the same due to the absence of a conventional military campaign were the cyber attacks against Ukrainian and NATO information systems during the recent Russian subversion and annexation of Ukraine's Crimea region. Indeed, across the spectrum of military operations it is reasonable to conclude that any future operation will include a cyber component.

These, then, represent a palate of threats that are growing, and no doubt even this short list is incomplete. The one thing we can say with near certainty: the threats are not going away but are becoming more commonplace and increasing in their sophistication. Now let's take a look at what nations and international organizations are doing to counter these threats.

4. Highlights of the US system for Critical Infrastructure protection

The US has matched a federal department to work with each of the sixteen sectors of critical infrastructure already mentioned. The majority of sectors are the responsibility of the Department of Homeland Security. Some sectors are matched to other departments, for example, the defense industrial sector is matched to the Department of Defense and the banking sector to the Department of the Treasury.

Each sector has a corresponding Information Sharing and Analysis Center or ISAC for public-private partnering and voluntary information sharing on threats and protection techniques. These are important exchanges because approximately 85% of US critical infrastructure is in the private sector, while the government side of these partnerships typically has better awareness of the overall threat than any of the individual private corporations or business sectors.

A National Infrastructure Protection Plan (NIPP) has been developed, along with a series of Sector Specific Plans (SSPs) to correspond with each identified sector. These are synchronized within a National Response Framework (NRF), an overall guide for how

the United States responds to all manner of disasters and emergencies, not only cyber space based crises.

In February 2014 President Obama unveiled the first voluntary cybersecurity standards for businesses to use in protecting the critical infrastructure they own. The standards also encourage greater information sharing across business sectors and with relevant government agencies. This is a first step. Getting competing companies to share information about successful attacks against them is difficult and potentially economically harmful. However, in time compliance should fall into place and ultimately perhaps a law requiring compliance might as well.

As part of its responsibilities to assist the defense industrial sector, the Department of Defense launched an Enhanced Cybersecurity Initiative to share threat and protection information with defense contractors regarded as part of that sector of critical infrastructure. Similar initiatives are assist other sectors are being developed by other departments, most notably the Department of Homeland Security.

Finally, the US 2011 International Strategy for Cyberspace commits to 'provide the necessary knowledge, training and other resources to countries seeking to build their own technical and cybersecurity capacity. US support ranges from supporting national capabilities for incident management to building public-private partnerships, to enhancing control system security, to drafting effective cyber crime laws. The US has worked with other counties individually and in fora under the auspices of the OAS, APEC, NATO and the UN.

5. Let us now look briefly at what is already being done by international organizations to protect infrastructure

The United Nations

The work of the UN's Group of Government Experts (the GGE) has been gaining credibility as one of the more encouraging efforts at international cooperation since 2004. GGE agreements in 2010 and 2012 have been modest yet noteworthy — as such enterprises usually are at the beginning. Each was more substantive than the last (the 2010 agreement followed an earlier failed attempt to reach an agreement) and we should be optimistic that the next round of discussions, though among a wider group of experts, will continue that trend. We need not say more here about the positive momentum of GGE because we are fortunate to have Ambassador

Andrey Krutskikh next on the plenary program. He is well known to all of us as one of the original GGE members, the chair of the 2012 GGE agreement, and a seasoned veteran who will again be negotiating this coming summer at the next round of discussions. No doubt Andrey will offer us some valuable insights into what to expect during the next and larger two year GGE enterprise. What is important here is to make clear that the UN is actively engaged in furthering international cyber security.

International Telecommunications Union

The ITU drafted its Global Cybersecurity Agenda (GCA) in 2007 with five pillars: a Legal Framework; Technical Measures; Organizations Structures; Capacity Building; and International Cooperation. The ITU is the lead global agent for confidence building measures in the ICT sector. One of its most visible projects is the Global Cybersecurity Index, which ranks cyber security capabilities of nation states based on the five criteria of Legal Measures, Technical Measures, Organizational Measures, Capacity Building and Cooperation. ITU partners with other organizations, such as: the UN Office of Drugs and Crime (UNODC) to share best practices in cybercrime legislation; the International Multilateral Partnership Against Cyber Threats (IMPACT) to work toward global solutions to cyber threats; and the Forum for Incident Response and Security Teams (FIRST) to share best practices on computer incident response capabilities.

European Union

The EU is perhaps the most active regional organization in international cyber security, which reflects its solid bureaucratic roots. In 2004 the EU established the European Network and Information Security Agency (ENISA) in Crete, which is celebrating its 10th anniversary this year. It also began looking at infrastructure protection in 2004, and organized an information sharing European Public-Private Partnership for Resilience (EP3R) in 2009. Early last year it adopted the EU Cyber Security Strategy, and in August 2013 it updated its European Program for Critical Infrastructure Protection (EPCIP), with the three work streams of Prevention, Preparedness and Response.

The EPCIP identifies four priority pan-European sectors: the EuroControl Air Traffic System; the Galileo global satellite navigation system; the Electricity Transmission Grid and the European Gas Transmission Network.

The EU has developed a Critical Infrastructure Warning Information Network (CIWIN), an Internet-based system for exchanging critical infrastructure protection ideas, studies and best practices among its members and their agencies. The CIWIN portal has been up and running since mid-January 2013. The EU's Digital Agenda for Europe has conducted, though ENISA, two pan-EU cyber security exercises examining critical infrastructure protection across the Union. It also set minimum baseline capabilities and services and policy recommendations for member's National/ Governmental Computer Emergency Response Teams (CERTs) to function effectively.

North Atlantic Treaty Organization (*NATO*)

NATO has been involved in Critical Infrastructure Protection (CIP) since 2001. In 2003 the Senior Civil Emergency Planning Committee adopted a six point plan to help nations manage the consequences of Chemical, Biological, Radiological and Nuclear (CRBN) attacks, particularly resulting from terrorism. In\2006 Heads of State and Government confirmed the Alliance role in CIP to protect its members' populations, territories, infrastructure, and forces from the consequences of terrorist attacks, and to protect its own security interest from the disruption in the flow of vital resources.

In 2011 the Alliance began to look at its dependencies on member critical infrastructures and work with members to assess the vulnerabilities to systems vital to Alliance missions and operations. In 2014 Alliance ministers are expected to approve a new Cyber Defense Policy that will strengthen NATO programs over the next several years.

More recently, indeed earlier this month on 5-8 April, the North Atlantic Council accepted the request of Ukraine, a NATO partner country, and sent the NATO Advisory Support Team on Critical Infrastructure and Civil Population Protection to assist Ukraine in developing civil contingency plans and crisis management measures. These related to critical energy infrastructure and risks to civil protection in the event of further aggravation of the security situation there.

Organization for Security and Cooperation in Europe (*OSCE*)

OSCE expressed consensus interest in cyber security as a transnational threat at its 2010 summit and again at a special conference convened on cybersecurity in 2011. In December 2013, the

OSCE agreed an "Initial Set of Confidence-Building Measures to Reduce the Risk of Conflict Stemming from the Use of Communications and Information Technologies (ICT)." This list includes, *inter alia,* the voluntary holding of consultations at an appropriate level in order to reduce the risk of misperception...and to protect critical national and international ICT infrastructures, including their integrity.

Organization for Islamic Cooperation (*OIC*)

The OIC is another regional organization taking steps to address critical infrastructure protection, although by coaching interested members to strengthen their capacities at the national level. The OIC stood up OIC CERT in 2008 and to date 19 of 57 OIC members CERTs have joined OIC CERT. They convene 2-5 conferences annually to share best practices, norms and threat indications. Only some of these discussions support critical infrastructure protection but it is a welcome start. Worldwide we should applaud even small steps and encourage their growth in substance and transparency. It should be taken advantage of by many more OIC members, most immediately Afghanistan as it strives to make its ICT infrastructure more reassuring to an economy struggling to gain more truly commercial, post-ISAF footing at the end of this year.

The African Union (*AU*)

In January 2012 the AU drafted a Convention on Confidence and Security in Cyberspace. The stated purpose of the Convention is to establish a credible framework for cyber security in Africa. This is a first encouraging step toward AU engagement in critical infrastructure protection. The Convention was to be adopted in January 2014 but that was not done due to privacy objections from Kenya. The next step is for Kenya to submit its written objections by May 2014.

The Organization of American States (*OAS*)

In 2004 OAS members approved a resolution that called on the Secretariat to begin working on cyber security issues with the goal of each member state having organized a CSIRT, and the OAS organizing its own CSIRT as a coordinating mechanism for regional initiatives in cyber security. The latest information available is that most OAS members had CSIRTs in 2011, indicating the program has been largely a success. It is not clear how active the OAS

CSIRT itself is in mentoring members or organizing future OAS assistance programs similar to OIC.

Association of Southeast Asian Nations (*ASEAN*)

Singapore Declaration of 2003 called for establishing an ASEAN Information Infrastructure and CERTs for all by 2005; Master Plan on ASEAN Connectivity of 2010; ASEAN ICT Master Plan (AIM) 2015 agreed in 2011; Members committed in 2012 to continue ASEAN CERT Incident Drills in support of the ASEAN Network Security Action Council (ANSAC); the 2005 Framework for Co-operation on Network Security was updated in 2013.

Asia Pacific Economic Cooperation (*APEC*)

APEC has agreed on a number of cyber security documents since 2002 including a Cyber Security Strategy in 2005 that recognized the importance of the security of communications infrastructure and particularly the Internet across the APEC region.

Shanghai Cooperation Organization (*SCO*)

In March 2013 the SCO signed agreements to combat the use or potential use of computer networks for terrorist, separatist or extremist's ends. While these agreements do not appear to be intended to address critical infrastructure protection in any collective way, they nonetheless indicate SCO's engagement in this field at the present time.

No doubt there are other initiatives worldwide and those present who can contribute to this list are encouraged to do so during discussion. Those just cited are illustrative of the degree to which the UN and many regional organizations are beginning to grapple with the permanent task of critical infrastructure protection. Are any of them doing all that is needed in their respective realms? I expect all would agree they can and must do more and do everything they are already doing to greater effect, to higher standards they internally seek. We should work with them and encourage them to move forward energetically, transparently and cooperatively.

6. Conclusion

This brief *tour d'horizon* of critical infrastructure and some of the protection initiatives already underway should whet your appetite for discussion and ideally new thinking on how to grapple with the associated challenges at the international level.

Let me seed such a discussion with three baskets of work that we should consider essential. First we must improve the resilience of our critical systems, new and old, and commit to investing in system improvements at a rate apace with or ahead of the bow wave of future risks we foresee. We must embrace this nationally through public-private enterprise, regionally, and globally.

We should also invest in curbing the ease with which the particular nemesis of botnets can be organized and promulgated, including by-hire networks for criminal use. This will require nations to take responsibility to deal with lawless behavior on their territory. It will also require improving the speed and excellence of network forensics and finding the means to employ Internet traffic filtering, most probably at the ISP level. There are many sound reasons why filtering has not been widely implemented — latency, cost, privacy, etc). We need solutions that satisfy the various stakeholders involved, including the ISPs and the users themselves.

Related to computer forensics, which is a broader field than the one example I just gave, and filtering policies, we need a far more educated and alert user workforce, one that in aggregate becomes far better at best practices and computer hygiene. This human dimension of critical infrastructure protection is too often overlooked. It is not where the money is for tech companies selling network security solutions. Yet, there is little doubt this is where the biggest security gap lies. Unwittingly, honest and authorized users simply allow their access credentials to be easily pirated away — from bad passwords to unauthorized devices on networks to unsecured authentication medium to succumbing to spear phishing. Will the next generation of users, the generation raised on-line, be better at security? Perhaps, but that is not readily apparent given the freedom with which personal information is shared on social media. It will take computer security being embedded in every method and subject of education. Technology of course can help by making security built-in by default.

Active defense and reconnaissance within critical information networks is another essential component of protection. Network administrators must be able to detect malware not only at boundary portals, but also within their network where hidden, unauthorized and untrusted agents will lurk, masquerading as authorized users and thus would be otherwise undetected.

Nor can we, as noting at the beginning of this discussion, ignore the physical threat to information systems, be it posed by a natural disaster like Hurricane Sandy, an act of terrorism or some other form of destruction. Just like cyberspace-based protection meas-

ures, physical protection measures must include fixed hardening, redundancy and suitable barriers, as well as dynamic protection such as active human or automated surveillance systems.

We will need to prioritize and invest sufficient resources so that over time protections become and remain adequate. We should address challenges on two fronts — at the user end-points on the networks, through training such as Stop-Think-Connect; and also strengthening protection at the key infrastructure nodes where we can shield millions of systems and IP addresses at once. We have to take both approaches and not simply invest in one or the other.

Finally we will need the capacity, connectivity and resilience to respond together in ways that achieve timely system recovery and limit the impacts of infrastructure failure. When we have put all these capabilities in place we will be well on our way, and well prepared, to meet the present and future challenges to critical infrastructure protection.

А.А.Стрельцов

Институт проблем информационной безопасности МГУ имени М.В.Ломоносова

Основные направления развития международного права вооруженных конфликтов применительно к киберпространству

Использование информационных и коммуникационных технологий (ИКТ) в качестве «силового» средства разрешения межгосударственных противоречий становится все более опасной угрозой международному миру и безопасности.

Как отмечено Группой правительственных экспертов ООН в 2013 году [1], «...Все страны заинтересованы в поощрении использования ИКТ в мирных целях. Страны также заинтересованы в предотвращении конфликтов, возникающих в результате использования ИКТ. Общее понимание в отношении норм, правил и принципов, применимых к использованию ИКТ государствами, и добровольные меры укрепления доверия могут играть важную роль в поддержании мира и безопасности».

Вопрос о правовом противодействии злонамеренному использованию ИКТ не является новым. Первые работы, посвященные проблематике применения международного права к киберпространству вообще и к Интернету в частности, появились еще в середине 90-х годов. Там не менее, поиск ответа на вопрос продолжается.

С одной стороны, по мнению многих специалистов, злонамеренное использование ИКТ способно нанести вред, иногда сравнимый с применением традиционного оружия, а в ряде случаев — с применением оружия массового уничтожения, и, с этой точки зрения, такое использование ИКТ представляет серьезную угрозу международному миру и безопасности и должно порождать неотъемлемое право государства на самооборону в смысле ст.51 Устава ООН.

С другой стороны, несмотря на «очевидность» возможности использования ИКТ в военных целях, практически все специалисты считают, что ИКТ не являются оружием. И в российской, и в англоязычной литературе термин «ИКТ» часто

[1] Доклад группы правительственных экспертов ООН. Представлен Генеральным Секретарем ООН 68-ой сессии Генеральной Ассамблеи ООН, 24 июня 2013 г., A\68\150

рассматривается как синоним понятия «информационные технологии». В англоязычной литературе он трактуется в более общем смысле как понятие, интегрирующее все телекоммуникационные средства, компьютеры, а в случае необходимости — специальное и общее программное обеспечение, память, системы аудио-, видеовизуализации, используемые пользователем для накопления, передачи, обработки информации.

С учетом этих двух обстоятельств, некоторые специалисты предлагают принять международный договор, позволяющий в ответ на злонамеренное использование ИКТ осуществлять контрмеры, выходящие за рамки ст.51 Устава ООН, но соответствующие положениям проекта Конвенции об ответственности государств за международно-противоправную деятельность. Проект данной Конвенции разработан комиссией по международному законодательству ООН, обсужден и принят к сведению Генеральной Ассамблеей ООН в 2001 году и, таким образом, не является источником права.

По мнению автора, устранение пробелов в терминологии, возникающих в нормах международного права при их применении к злонамеренному использованию ИКТ, а также пробелов в правовом регулировании международных отношений, связанных со злонамеренным использованием ИКТ в качестве средства ведения «силового» противоборства между государствами для достижения политических задач, может быть осуществлено в рамках адаптации международного права вооруженных конфликтов.

В этом случае адаптация должна затронуть две относительно самостоятельные части международного права вооруженных конфликтов:

- право применения силы (Jus ad Bellum), определяющее условия, при которых сила может быть применена государством в международных отношениях, включая обеспечение самообороны;
- право ведения войны (Jus in Bello), определяющее правила применения государством и негосударственными образованиями вооруженной силы в процессе международных и немеждународных конфликтов, в том числе соблюдения ограничений гуманитарного характера.

Отдельным вопросом, требующим обсуждения, является возможная форма закрепления правовых новаций в международных договорах.

1. Международное право Jus ad Bellum. Основным источником права Jus ad Bellum является Устав ООН, который закрепля-

ет базовые нормы, регулирующие отношения в области применения и угрозы силы, и, одновременно, ограничивает действие в данной области обычных норм международного права.

Как следует из ст. 41 и 42 Устава ООН, выделяют два основных вида «силы» — сила, связанная с использованием вооруженных сил (оружия) и сила, не связанная с использованием оружия.

Сила, связанная с использованием вооруженных сил, заключается в принуждении одного государства к исполнению воли другого государства посредством создания для принуждаемого государства безвыходной ситуации под угрозой физического уничтожения его политического руководства, государственного аппарата, оружия, вооруженных сил, техники, разрушения экономической основы существования, причинения страданий гражданскому населению, т.е. методом непосредственного насилия.

Сила, не связанная с использованием вооруженных сил, реализуется посредством полной или частичной «изоляции» принуждаемого государства, прерывающей пути его общения с другими государствами. Эта изоляция может проявляться в форме перерыва экономических отношений, железнодорожных, морских, воздушных, почтовых, телеграфных, радио- и других средств сообщения, а также разрыва дипломатических отношений.

Как известно, ИКТ, являясь фактором производства и повышения качества жизни граждан, обеспечения функционирования объектов инфраструктуры общества и государства, могут быть использованы в качестве средства негативного воздействия на различные сферы жизнедеятельности общества и государства, на развитие экономических, социальных, культурных и политических отношений. Негативное воздействие ИКТ в некоторых случаях может приводить к человеческим жертвам (воздействие на автоматизированные системы управления авиационным, железнодорожным и автомобильным сообщением, на систему управления электроснабжением и т.д.), значительным разрушениям (воздействие на системы автоматизированного управления технологическими процессами в гидро-, электро-, атомных станциях), нанесению ущерба экономическому, военному, оборонному потенциалу государства и общества.

Злонамеренное использование ИКТ при определенных обстоятельствах может рассматриваться как угроза силой или ее применение против территориальной целостности или политической независимости государства — жертвы. При этом

ИКТ могут также быть использованы в качестве средства насилия, не связанного с применением вооруженных сил. Это обусловлено тем, что технологической основой реализации функций международного информационного обмена в современном мире является глобальная сеть Интернет. С этой точки зрения одной из форм «изоляции» государства может быть прерывание оказания услуг в области передачи, хранения, обработки, поиска и распространения информации в сети Интернет. Возможность осуществления таких действий в рамках реализации мер по поддержанию или восстановлению международного мира и безопасности, не связанных с использованием вооруженных сил, по существу содержится в положениях ст. 41 Устава ООН, закрепляющей возможность перерыва и «других средств сообщения».

Как следует из изложенного, международные отношения в области злонамеренного использования ИКТ в основном урегулированы нормами ст. 2 (4) Устава ООН, предъявляющими к государствам требование воздерживаться от угрозы силой или ее применения в международных отношениях, в том числе и в киберпространстве.

В то же время, по мнению автора, возможно правовое закрепление признаков злонамеренного использования ИКТ, достигающего порогов «угрозы применения силы» и «применения силы».

В качестве такого порога для «применения силы» может рассматриваться наступление серьезных последствий злонамеренного использования ИКТ, т.е. факты реального навязывания воли другому государству, принуждения к изменению его политики в области «территориальной целостности», «политической независимости» или иных ценностей, укрепление которых составляет Цели ООН.

Пороговым признаком «угрозы применения силы» может являться предупреждение официальных лиц государства о возможности применения силы в форме злонамеренного использования ИКТ, практическая демонстрация накопленного потенциала ИКТ для достижения преследуемых политических целей, не достигающего порога «применения силы».

В современном международном праве, по существу, единственным условием легитимного применения силы государством является его самооборона в ответ на вооруженное нападение. Неотъемлемое право на индивидуальную и коллективную самооборону при вооруженном нападении закреплено ст. 51 Устава ООН.

Термин «вооруженное нападение» применительно к Jus ad Bellum может раскрываться как:

- «применение силы», воздержание от которого требуют положения ст. 2 (4) Устава ООН;
- агрессия, т.е. применение вооруженной силы государством против суверенитета, территориальной неприкосновенности или политической независимости другого государства, или каким-либо другим образом, несовместимым с Уставом Организации Объединенных Наций.

С этой точки зрения, агрессия, совершенная посредством злонамеренного использования ИКТ, могла бы служить основанием для возникновения права индивидуальной или коллективной самообороны при условии, что между ИКТ и «оружием» в традиционном смысле слова существует однозначное соответствие, т.е. ИКТ являются разновидностью «оружия».

Как уже отмечалось, «процессы» и «методы» не являются ни «устройствами», ни «средствами» и, с этой точки зрения, не могут быть отнесены к оружию. В то же время ИКТ могут быть использованы для изменения нормального («штатного») режима функционирования информатизированных объектов и устройств, приводящего к возникновению реальной угрозы жизни и здоровью людей, сохранности зданий и сооружений, сохранению экологии, т.е. превращению данных объектов и устройств в «оружие». Именно возможность превращения обычных (неспециализированных) устройств в оружие вследствие нештатного их применения была использована террористами при осуществлении атак 11 сентября 2011 г. в США. Эти обстоятельства при поддержке со стороны международного сообщества позволили правительству США объявить о своем праве на индивидуальную и коллективную самооборону и начать вооруженные действия против Ирака и Афганистана, обвиненных в поддержке террористов.

Таким образом, террористическая атака 11 сентября 2001 г. с использованием захваченных террористами самолетов была де-факто приравнена к «вооруженному нападению» в смысле ст. 51 Устава ООН. Очевидно, что при этом несколько расширяется трактовка понятия «оружия», которая стала включать в себя устройства, которые при определенных обстоятельствах приобретают свойства «оружия».

Злонамеренное использование ИКТ можно рассматривать в качестве фактора, способного превращать обычные (невоенные) устройства в такие, которые предназначены для поражения живой силы и техники противника, т.е. в «оружие».

Такую разновидность оружия можно обозначить понятием «неявное оружие».

Злонамеренное использование ИКТ превращает тот или иной объект или устройство в «неявное оружие» в случае, если объект обладает следующим свойствами:

- способностью наносить ущерб (поражение) живой силе и технике при нарушении нормального (штатного) режима их функционирования;
- наличием в составе устройства или объекта информационных или коммуникационных систем, способных обеспечить реализацию злонамеренного использования ИКТ, приводящего к поражению живой силы и техники;
- наличием ИКТ, предназначенных для превращения невоенного устройства или объекта в «неявное оружие».

При таком подходе любое нападение, осуществленное с использованием так называемого «неявного оружия», является вооруженным нападением и порождает следствия, предусмотренные ст. 51 Устава ООН.

Исходя из этого, вообще говоря, положения ст. 51 Устава ООН не требуют адаптации к условиям злонамеренного использования ИКТ в киберпространстве.

Одной из важных особенностей использования ИКТ в качестве средства применения угрозы силы или ее применения в смысле ст.2 (4) Устава ООН, а также осуществления вооруженного нападения в смысле ст. 51 Устава ООН является ее ненаблюдаемость для человека. Это обусловлено тем, что ИКТ — есть, вообще говоря, процесс целенаправленного изменения, в соответствии с определенным алгоритмом, информации, хранящейся в элементах электронной памяти компьютеров, средств связи и коммуникационных устройств.

Это осложняет оценку объективности данных, приводящихся участниками спора по поводу нарушения международного права посредством злонамеренного использования ИКТ.

Для справедливого рассмотрения таких споров представляется важным создать единую систему (возможно на базе соответствующих национальных и региональных систем) регистрации фактов угрозы силой или ее применения, а также «вооруженного нападения» посредством злонамеренного использования ИКТ. При этом национальные и региональные элементы системы регистрации должны быть сертифицированы по единым стандартам, а обслуживающий эти устройства персонал — обладать правом экстерриториальности под эгидой ООН.

2. Международное право Jus in Bello. Основными источниками права в рассматриваемой области являются Гаагские конвенции, Женевские конвенции и другие международные договоры, подписанные в развитие норм и идей данных конвенций. Как известно, международное гуманитарное право регулирует отношения, связанные с уменьшением физических страданий лиц, непосредственно затронутых военными действиями, ущерба имуществу гражданского населения, а также с обеспечением сохранности культурных ценностей.

С учетом изложенной выше концепции «неявного оружия», нормы гуманитарного права регулируют общественные отношения, связанные со злонамеренным использованием ИКТ в киберпространстве для достижения военно-политических целей. Несмотря на общие черты, имеющиеся у ИКТ с «традиционным оружием» в способах причинения насилия, в видах страданий раненых, больных, гражданского населения, а также в формах нанесения ущерба культурным ценностям, в правовом регулировании рассматриваемых общественных отношений имеются и существенные различия.

Как показал анализ, основная часть положений, закрепленных в источниках международного гуманитарного права, либо инвариантна к виду оружия, используемого в процессе военных действий, либо ориентирована на ограничение использования конкретных видов вооружения. Так, правила ведения военных действий и ограничения на средства решения военных задач почти не зависят от вида оружия, а нормы, запрещающие использование некоторых видов вооружения, регулируют отношения, связанные с использованием именно этих вооружений.

В то же время ряд норм международного гуманитарного права требуют адаптации к условиям злонамеренного использования ИКТ. Это связано, прежде всего, с тем, что ИКТ являются объектами урегулированных международными договорными актами международных отношений, связанных с распространением и передачей информации. Злонамеренное использование ИКТ может помешать надлежащему выполнению международных договоров, например, предусматривающих создание и ведение реестров, справочников. Кроме того, использование ИКТ в качестве средства трансформации невоенных объектов в военные также могут стать предметом международных ограничений их применения в военных действиях.

К числу норм международного гуманитарного права, требующих адаптации, в первую очередь, относятся нормы, регулирующие международные отношения в следующих областях:

- опознавания;
- запрета некоторых случаев злонамеренного использования ИКТ в военных целях;
- вероломства;
- шпионажа и разведки;
- сохранения нейтралитета государств, не участвующих в военных действиях.

Права и обязанности нейтральных государств регулируются нормами международного гуманитарного права нейтральных держав и лиц в случае сухопутной и морской войн. Как представляется, одной из наиболее сложных проблем в осуществлении правоприменительной практики воюющими государствами в отношении злонамеренного использования ИКТ против нейтральных государств является идентификация, прежде всего, критически важных объектов их национальных информационных инфраструктур, позволяющая предотвратить в отношении этих государств случайное или намеренное нарушение норм международного права.

Представляется, что решение данной задачи может быть осуществлено посредством составления карт цифровых адресов критически важных объектов национальных информационных инфраструктур нейтральных государств и передача их в случае начала вооружённого конфликта воюющим сторонам, а также мониторинга случаев злонамеренного использования ИКТ против объектов, указанных в карте.

Кроме того, было бы целесообразно создать единый орган по координации противодействия опасной деятельности государств против критически важных объектов глобальной, региональных и национальных информационных инфраструктур, наподобие Международного органа по морскому дну.

Работу создаваемого органа было целесообразно строить на основе Правил поведения государств в области международной информационной безопасности. Проект таких правил представлен в 2011 году Российской Федерацией, Китаем, Таджикистаном, Узбекистаном в ООН.

3. Предложения по форме закрепления адаптированных правовых норм и порядку их введения в действие. Важным фактором решения задачи адаптации международного права вооруженных конфликтов является правовое оформление предлагаемых правовых новаций. В основу деятельности по совершенствованию международного права, как на основе принципа кодификации, так и на основе принципа прогрессивного развития лежат международные принципы друже-

ственных отношений и сотрудничества. К числу этих принципов относится обязанность сотрудничать друг с другом в соответствии с Уставом ООН, без применения которого невозможно предложить справедливый подход к формальному закреплению правовых новаций в области адаптации международного права вооруженных конфликтов.

Одним из рациональных подходов к выполнению рассматриваемой задачи является подготовка проектов приложений к международным договорам, регулирующим международные отношения в области вооруженных конфликтов применительно к злонамеренному использованию ИКТ. Как известно, количество источников международного права в данной области, требующих адаптации, сравнительно невелико. Соответственно, работу по подготовке проектов международных договоров можно было бы организовать в форме подготовки системы относительно независимых материалов, объединенных единой терминологией и принципами. Разработку каждого проекта договора можно было бы проводить, придерживаясь той терминологии и с сохранением тех правовых механизмов, которые уже выдержали проверку как на уровне международных экспертов и политиков, так и временем.

К числу таких проектов международных договоров можно было бы отнести следующие:

- соглашение о порядке применения положений статей 2(4), 39, 41, 42 и 51 Устава ООН к случаям применения силы или угрозы применения силы посредством злонамеренного использования ИКТ, предусмотрев в нем вопросы создания международной системы взаимопомощи в области расследования вооруженных нападений с использованием ИКТ;
- соглашение о дополнительной охране реестров и списков, создаваемых в соответствии с нормами международного гуманитарного права, от атак со злонамеренным использованием ИКТ;
- соглашение о создании международной системы регистрации информационных систем объектов и лиц, защищаемых международным гуманитарным правом, а также международной системы мониторинга нарушения норм международного гуманитарного права в отношении этих объектов и лиц;
- соглашение о добровольном ограничении шпионской и разведывательной деятельности в киберпространстве;
- соглашение об уточнении порядка идентификации объектов информационного пространства, защищаемых международным гуманитарным правом;

• соглашение о запрещении злонамеренного использования ИКТ против критически важных объектов глобальной, региональных и национальных инфраструктур, подпадающих под защиту международного права;
• соглашение о создании и ведении реестра критически важных объектов глобальной, региональных и национальных инфраструктур, нападение на которые со злонамеренным использованием ИКТ является международным преступлением.

Выводы

Одним из важных направлений прогрессивного развития современного международного права вооруженных конфликтов является его адаптация к условиям злонамеренного использования ИКТ в военных целях.

Выполнение данной задачи предлагается осуществлять по трем основным направлениям: адаптации международного права применения силы; адаптации международного гуманитарного права; совершенствования международного процедурного права.

В основу адаптации международного права применения силы может быть положена концепция «неявного оружия», позволяющая минимизировать появляющиеся правовые новации и сохранить жесткие границы легального применения силы, установленные ст. 51 Устава ООН.

В рамках адаптации международного гуманитарного права к злонамеренному использованию ИКТ правовые новации затрагивают большой объем международных отношений, связанных как с расширением перечня запрещенных видов оружия и способов его использования, так и с идентификацией в информационном пространстве объектов и лиц, находящихся под защитой норм международного права.

Совершенствование процедурной части международного права вооруженных конфликтов затрагивает, в основном, вопросы объективизации юридических фактов, обусловливающих возникновение, прекращение или изменение правоотношений, связанных с использованием ИКТ в качестве средства «силового» разрешения межгосударственных противоречий.

Dr. A.A.Streltsov

Institute of Information Security Issues, Lomonosov Moscow State University

Focal Areas in Development of International Law of Armed Conflict in the Context of Cyberspace

The use of information and communication technologies (ICTs) as a "coercive" tool for resolving international conflicts is becoming an increasingly perilous threat to international peace and security.

According to the 2013 UN Group of Governmental Experts, "It is in the interest of all States to promote the use of ICTs for peaceful purposes. States also have an interest in preventing conflict arising from the use of ICTs. Common understandings on norms, rules and principles applicable to the use of ICTs by States and voluntary confidence-building measures can play an important role in advancing peace and security."

Legal countermeasures to malicious use of ICTs represent an issue that is not new on the agenda. The original papers on the use of international law in the context of cyberspace in general and in the Internet in particular were published back in the middle of the 1990s. Nonetheless, experts still keep looking for answers.

On one hand, many experts believe that malicious use of ICTs may cause damage that may be compared, in certain circumstances, with the use of conventional weapons, and in some cases even with the use of weapons of mass destruction. From this perspective, such use of ICTs represents a major threat to international peace and security and shall engender the right of self-defense for a state in terms of Article 51, UN Charter.

On the other hand, despite the "obvious" possibility of using ICTs for military purposes, almost all the experts presume that ICTs are not a weapon. In both Russian-language and English-language literature, the term "ICTs" is often regarded as a synonym to "information technologies." In the Russian laws, the term "information technologies of such processes and methods". In the English-language literature, this term has a broader meaning and stands for a concept that integrates all the existing telecommunications, computers, and, where necessary, any special and general-purpose software, memory, and audio-visual systems, which users may employ to store, transmit and process information.

In recognition of these two aspects, some experts propose adoption of an international treaty that would enable us to take countermeasures, in response to the malicious use of ICTs, that would be outside the scope of Article 51, UN Charter, but would nevertheless comply with the provisions of Draft Convention on the Responsibility of States for Internationally Wrongful Acts. This Draft Convention was developed by the UN Inernational Law Commission, discussed and taken note of by the UN General Assembly in 2001, and therefore does not represent a source of law.

The author of this article believes that the process of customizing the international law of armed conflict may include bridging the gaps in terminology that develop in the norms of international law when applied to the malicious use of ICTs, as well as bridging the gaps in legal regulation of international relations where malicious use of ICTs represents a tool of power struggle between states seeking to pursue certain political objectives.

In this case, customization shall involve two relatively independent segments of international law of armed conflict:

- Law on the use of force (Jus ad Bellum), which determines when a state can use force in the context of international relations, including for the purpose of self-defense, and
- Law of warfare (Jus in Bello), which determines the rules for the use of armed force by the state and non-state entities in the course of international and non-international conflicts, to include the rules applicable to humanitarian constraints.

A separate issue that needs discussion is the format that can be used to document legal innovations in international treaties.

1. Inernational law Jus ad Bellum. The primary source of Jus ad Bellum law is the UN Charter, which lays down the basic rules for regulating relations based on the use of force or threat of force and, at the same time, restricts application of conventional rules of international law in this domain.

According to Articles 41 and 42, UN Charter, there are two basic kinds of "force": force that implies the use of armed forces (weapons), and force that does not imply the use of weapons.

In case of force that implies the use of armed forces, one state coerces another state to act as the coercing state desires by pushing the coerced state into a deadlock at threat of physical elimination of its political leadership, political machinery, weapons, armed forces and equipment, destruction of the economic foundation of existence, and infliction of suffering on the civil population, i.e. through the use of direct violence.

In case of force that does not imply the use of armed forces, the state being coerced is "isolated," whether partially or completely, to disallow communication with other states. Such isolation may take the form of interruption of economic relations, communications by rail, sea, air, via mail, telegraph, radio and other means of communication, and in the form of severance of diplomatic relations.

As we know, ICTs, being one of the factors that promote industry and standard of living and enable operation of public and national infrastructures, may be used as a tool for damaging various living environments of the society and the state and for harming the economic, social, cultural and political relations. In some cases, such adverse impact of ICTs may result in fatalities (impact on automated control systems in aviation, railway and highway sectors, power supply control system, etc.), significant destructions (impact on automated process control systems used at hydro power plants and nuclear plants), and damage to the economic, military, and defense capabilities of the society and the state.

Malicious use of ICTs may be considered, in a number of circumstances, as threat of force or use of force against the territorial integrity or political sovereignty of the state being affected. Besides, ICTs may also be used as a means of violence that does not imply the use of armed forces. This is due to the fact that information exchange function is implemented through the Internet in the modern world. From this perspective, interruption of data transmission, storage, processing, retrieval and distribution services using the Internet may be one of the ways to "isolate" a state. Recourse to such actions (which do not imply the use of armed forces) within the context of measures intended to maintain or restore international peace and security is essentially stipulated by the provisions of Article 41, UN Charter, which provides for potential interruption of "other means of communication."

It therefore appears that international relations in the domain of malicious use of ICTs are generally governed by the provisions of Article 2 (4), UN Charter, which require states to abstain from the use of force of threat of force in international relations, including in cyberspace.

At the same time, the author believes there is an opportunity for legal confirmation of the criteria of malicious use of ICTs at the borderline of "threat of force" and "use of force."

For the "use of force," such borderline may be represented by the onset of severe effects of malicious use of ICTs, i.e. actual enforcement of will on another state, coercion to change its policy as

regards its territorial integrity, political sovereignty or other values that a state shall seek to consolidate in accordance with the UN goals.

A borderline of "threat of force" may be represented by warning of a state's public officers about potential use of force in the form of malicious use of ICTs, as well as practical demonstration of accumulated ICT resources intended to pursue the political goals that do not reach the "use of force" borderline.

In principle, the only reason for legitimate use of force by a state provided by the modern international law is self-defense in response to an armed assault. Indefeasible right to individual and collective self-defense in case of armed assault is provided by Article 51, UN Charter.

The term "armed assault" relating to Jus ad Bellum may be construed as:

- "use of force" that a state shall refrain from in pursuance of provisions of Article 2 (4), UN Charter, or
- aggression, i.e. use of armed force by a state against the sovereignty, territorial integrity or political independence of another state, or use of armed force by any other means contradictory to the UN Charter.

From this point of view, aggression committed by means of malicious use of ICTs could constitute grounds for the creation of right to individual or collective self-defense, provided that ICTs and the term "weapon" in its conventional meaning are synonymous, i.e. ICTs are a type of "weapon."

As stated above, "processes" and "methods" are neither "devices," nor "tools," which means they cannot be treated as weapons in this context. At the same time, ICTs may be used to change the regular ("nominal") operation of computerized facilities and devices, leading to a real threat to life and health of people, integrity of buildings and structures, and environmental security, i.e. conversion of such facilities and devices into "weapons." It is the possibility to convert conventional (non-specialized) devices into weapons as a result of their off-nominal application was used by terrorists during the attacks in the USA on September 11, 2001. These considerations, with support of the international community, enabled the US government to announce its right to individual and collective self-defense and engage in military operations against Iraq and Afghanistan — countries accused of support of terrorism.

As a result, the 9/11 terrorist attack, in which terrorists used hijacked planes, was de facto made equal to an "armed assault" in the meaning of this term provided by Article 51, UN Charter.

Apparently, the term "weapon" therefore shall now have a broader meaning, to include devices that have the properties of "weapon" in certain circumstances.

Malicious use of ICTs may be viewed as a factor that may turn conventional (non-military) devices into those employed for killing enemy troops and hardware, i.e. "weapons." This type of weapons can be called "implicit weapons."

Malicious use of ICTs transforms a facility or device into "implicit weapon" if such facility or device has the following properties:

capability to injure (damage) troops and hardware as a result of failure of their regular (nominal) operation;

existence of information or communication systems within a facility or device that enable malicious use of ICTs resulting in damages of troops and hardware;

existence of ICTs intended to transform a non-military device or facility into an "implicit weapon."

From this perspective, any assault involving the so-called "implicit weapons" shall be deemed as an armed assault and lead to implications stipulated by Article 51, UN Charter.

To this end, generally speaking, provisions of Article 51, UN Charter do not require customization to the conditions of malicious use of ICTs in cyberspace.

One of the important features of using ICTs for threat of force or for use of force in the meaning provided by Article 2 (4), UN Charter, and for the purpose of an armed assault in the meaning provided in Article 51, UN Charter is its unobservability. This unobservability is due to the fact that ICTs basically represent a process of purposeful change, in accordance with a certain algorithm, of information stored in electronic memory of computers, means of communication, and communication devices.

This fact makes it harder to assess credibility of data presented by the debating parties with respect of breach of international law by way of malicious use of ICTs.

To enable fair consideration of such disputes, it appears vitally important to establish a unified system (possibly based on appropriate national and regional systems) for registering the cases of threat of force or use of force, as well as "armed assault" with the help of malicious use of ICTs. National and regional elements of the registration systems hall be certified in accordance with uniform standards, and the personnel operating such devices shall have the extraterritorial right under the aegis of the UN.

2. International law Jus in Bello. The primary sources of law in this domain include the Hague conventions, Geneva conventions, and other international treaties concluded to promote the rules and ideas of the stated conventions. It is commonly known that international humanitarian law regulates relations intended to reduce physical suffering of persons immediately affected by military operations and damage to property of civilian population, as well as to ensure integrity of cultural property.

Considering the concept of "implicit weapons" described above, the rules of humanitarian law regulate public relations that involve malicious use of ICTs in cyberspace in pursuit of military and political objectives. Despite the similarities between the ICTs and "conventional weapons" as regards the methods of violence, types of suffering of injured and sick persona and civilian population, as well as the forms of damage to cultural property, there are some major differences between them in terms of legal regulation of the subject public relations.

Based on our review, the majority of provisions contained in the sources of international humanitarian law are either invariable with regards to the type of weapon used during military operations, or implies restricted use of specific types of weapons. For instance, the rules of warfare and restriction of combat mission resources barely depend on the type of weapons used, and rules that prohibit the use of certain types of weapons regulate relations that imply the use of these specific weapons.

At the same time, certain rules of international humanitarian law require customization to the conditions of malicious use of ICTs. This is primarily due to the fact that ICTs are subjects of international relations governed by international treaties that involve distribution and communication of information. Malicious use of ICTs may obstruct due performance of international treaties, for instance those that provide for the development and maintenance of registers and reference books. Additionally, the use of ICTs as a means of transformation of non-military facilities into military facilities may also be subject to international restriction of their use for purposes of war.

The rules of international humanitarian law that require customization include, first of all, the rules that regulate international relations in the following domains:

- identification;
- prohibition of certain cases of malicious use of ICTs for purposes of war;
- perfidy;

- espionage and reconnaissance;
- retention of neutrality of states that do not participate in military operations.

Rights and duties of neutral states are governed by the rules of international humanitarian law of neutral powers and persons in war on land and naval war. It appears that one of the greatest challenges in law enforcement practices of belligerent states with respect of malicious use of ICTs against neutral states is identification, in the first place, of critical facilities of their national information infrastructures to help prevent accidental or deliberate breach of rules of international law with respect of such states.

In our opinion, this problem may be solved by compiling the charts of digital addresses of critical facilities of national information infrastructures of neutral states and communicating them, in case of armed conflict, to the belligerents, as well as by monitoring the cases of malicious use of ICTs against the facilities specified in the chart.

Besides, it might help to create a single authority to coordinate countermeasures against dangerous activities of states aimed at critical facilities of the global, regional and national information infrastructures similar to the Inernational Seabed Authority.

Such new authority could operate in reliance on the Rules of Conduct of States in Inernational Information Security. A draft document containing such rules has been presented in 2011 by the Russian Federation, China, Tajikistan and Uzbekistan in the UN.

3. Proposals on the form of securing the customized rules of law and procedure of their enactment. Legal registration of proposed rules of law is critical to the customization of international law of armed conflict. Activities aimed at improving the international law, based both on the codification principle and the progressive development principle, rely on the international principles of friendly relations and cooperation. These principles include the obligation of states to cooperate with each other in accordance with the UN Charter, without which there can be no fair approach to the official documentation and registration of legal innovations as regards the customization of international law of armed conflict.

One of the reasonable approaches to solving this problem involves the development of draft proposals to international treaties that regulate international relations with respect of armed conflicts in the context of malicious use of ICTs. It is common knowledge that the number of sources of international law in this domain that require customization is relatively small. Therefore, development of draft international treaties could be materialized in the develop-

ment of a system of relatively independent materials with common terminology and principles. Each draft treaty could be developed in reliance on the terminology and with retention of the legal mechanics that have already stood the test of time and demonstrated success on the level of international experts and politicians.

Such international treaties could include the following:

- Treaty on the application of provisions of Articles 2(4), 39, 41, 42 and 51 of the UN Charter to the cases of use of force or threat of force by means of malicious use of ICTs — with due consideration for the issue of establishment of international system of collaboration in investigations of armed assaults with the use of ICTs;
- Treaty on additional measures to secure registers and lists created in accordance with the rules of international humanitarian law against attacks involving the malicious use of ICTs;
- Treaty on the development of international system for registration of information systems of facilities and persons protected by the international humanitarian law, as well as the international system of monitoring violations of rules of international humanitarian law with respect of such facilities and persons;
- Treaty on voluntary restriction of espionage and reconnaissance in the cyberspace;
- Treaty on detailing the procedure of identification of information space objects protected by the international humanitarian law;
- Treaty on the prohibition of malicious use of ICTs against critical facilities of global, regional and national infrastructures protected by the international law;
- Treaty on the creation and maintenance of a register of critical facilities of global, regional and national infrastructures, assault on which with malicious use of ICTs constitutes an international crime.

Conclusions

One of the essential focal areas of progressive development of contemporary international law of armed conflict is customization of such law to the conditions of malicious use of ICTs for purposes of war.

Three core lines of customization are proposed: customization of international law of use of force; customization of international humanitarian law; and improvement of international law of procedure.

The process of customization of international law of use of force may be based on the concept of "implicit weapon," which allows

minimizing the emerging legal innovations and maintaining the tight limits of legitimate use of force, as stipulated by Article 51 of the UN Charter.

In the context of customization of international humanitarian law to malicious use of ICTS, legal innovations involve a significant scope of international relations that imply both expansion of the list of prohibited types of weapons and identification in the information space of facilities and persons protected by the rules of international law.

Improvement of the procedural aspect of international law of armed conflict mostly touches upon the issues of objectification of legal facts that underlie the emergency, termination or change of legal relations that involve the use of ICTs as a means of "coercive" resolution of international conflicts.

Гао Хуэй (Gao Hui)

Центр киберинформации при Китайском обществе дружбы с зарубежными странами (КОДЗС), КНР

Применимость права вооруженного конфликта в киберпространстве

Уважаемые гости!

Дамы и господа!

Для меня большая честь принять участие в вашей дискуссии по кибербезопасности в этом красивом альпийском городе. В этом году исполняется 20-лет с момента, как Китай вошел в Интернет. За последние 20 лет мы стали свидетелями стремительного развития Китая и значительных успехов в этой области. К концу 2013 года в Китае было 0,6 млрд. пользователей Интернета, половина из которых имеет опыт покупок онлайн. В первую десятку международных Интернет-компаний входят три китайских предприятия. Таким образом, Китай стал одной из ведущих держав в киберпространстве, и верным защитником кибербезопасности. Не так давно центральное правительство Китая создало руководящую правительственную группу по кибербезопасности и информатизации под руководством председателя КНР Си Цзиньпина. Мы твердо верим, что обеспечивать кибербезопасность Китаю необходимо совместно с международным обществом. Китайское общество дружбы с зарубежными странами (КОДЗС) стремится к развитию дружеского общения между Китаем и остальным миром, и мы также являемся одним из членов-учредителей Международного исследовательского консорциума информационной безопасности. Для того чтобы способствовать развитию международного сотрудничества в киберпространстве, КОДЗС создал специальный Кибер и информационный центр, и пригласил в качестве научных сотрудников множество первоклассных китайских экспертов по кибербезопасности и связанным с ней правовым вопросам. Мы хотели бы воспользоваться этой возможностью, чтобы активизировать сотрудничество с представителями и экспертами аналитических центров, присутствующих здесь сегодня.

Теперь я хотела бы поделиться некоторыми своими мыслями о применимости права вооруженного конфликта в киберпространстве.

Право вооруженного конфликта (ПВК), как правило, относится к *jus in bello* или международному гуманитарному праву. Но в более широком смысле оно может быть использовано для обозначения как *jus in bello*, так и *jus ad bellum*. В настоящем докладе эта концепция используется в более широком смысле.

I. Проблемы применения ПВК в киберпространстве

Jus ad bellum как правило, отражено в статьях 2(4) и 51 Устава ООН. Статья 2(4) запрещает угрозу силой или применения силы в международных отношениях, в то время как статья 51 позволяет государству, подвергшемуся вооруженному нападению, реализовать право на индивидуальную или коллективную самооборону. Отметим, что «применение силы» и «вооруженное нападение» — это два разных понятия. Хотя в Уставе ООН нет определения этих двух понятий, из текста мы можем увидеть, что государство может реализовать право на самооборону только тогда, когда применение силы достигнет масштаба «вооруженного нападения».

Jus in bello в основном отражено в Женевских конвенциях 1949 года и дополнительных протоколах к ней 1977 года, в том числе основных правилах и принципах, которые должны соблюдаться сторонами во время вооруженного конфликта. Есть четыре фундаментальных принципа, лежащих в основе *jus in bello*, а именно: военная необходимость, гуманность, принципы различия и соразмерности. Целью принципов является достижение баланса между военной необходимостью и гуманностью, для сведения к минимуму страданий, вызванных вооруженным конфликтом, без снижения боеспособности.

По моему мнению, для успешной реализации ПВК в киберпространстве, необходимо преодолеть многие проблемы и препятствия. Во-первых, что касается *jus ad bellum*, проблема признания операций в киберпространстве применением силы или вооруженным нападением, выявляет многие вопросы. Каково правильное пороговое значение «применения силы» и «вооруженного нападения» в киберпространстве? Когда в отношении кибератаки может быть реализовано право на самооборону? Каким образом в интересах самообороны можно противостоять атаке? Как осуществляя контратаку соблюдать требования «необходимости и соразмерности»? Являются ли хакеры законной целью? На самом деле, хотя некоторые

страны утверждают, что государство может воспользоваться правом на самооборону или даже подготовительную самооборону для противодействия неизбежным киберугрозам, они в то же время отмечают, что «деятельность в киберпространстве, которая косвенно приводит к гибели, травмам или значительным разрушениям, вероятно, будет рассматриваться как применение силы».

Во-вторых, что касается *jus in bello*, хотя обычное международное право и вводит некоторые ограничения относительно развития новых технологий в оружие, трудно сказать, что принципы различия и пропорциональности автоматически применимы в киберпространстве. С правовой точки зрения, необходимо дальнейшее исследование и анализ; с технической точки зрения, необходимо убедиться, что кибератаки являются управляемыми, можно реализовать требования принципов избирательности и соразмерности, и точно оценить возможный сопутствующий ущерб. Также проблемы возникают, когда в киберпространстве применяются другие нормы *jus in bello*, такие, как право нейтралитета.

II. Источники проблем и препятствий

Во-первых, киберпространство является виртуальным, взаимосвязанным пространством, в котором можно легко скрыть свою личность. Таким образом, киберпространство довольно сильно отличается от реального мира. Когда мы пытаемся применять нормы ПВК, разработанные для реального мира в киберпространстве, мы должны учитывать его особенности.

Во-вторых, понятия, связанные с кибер-, неоднозначны и не имеют общего понимания, в том числе кибервойна, киберпреступность, кибероружие, кибербезопасность и т.д. В этом смысле абсолютно необходимо определить относящиеся к теме термины и понятия.

В-третьих, нет критерия для оценки ущерба, причиненного кибератаками. Большинство толкователей используют критерий «прямой физической травмы и материального ущерба в результате действия в киберпространстве», но он не вполне понятен. Кроме того, кибероперации причиняют нефизический ущерб, который также должен быть принят во внимание. Однако до сих пор нет консенсуса по вопросам, может ли нефизический ущерб являться применением силы и как оценить этот ущерб.

В-четвертых, по-прежнему трудно осуществлять атрибуцию кибератак. В целом, это техническая проблема, которая включает в себя трудности определения источников атаки,

личности и намерений злоумышленника, отношений между атакующим и его государством. С правовой точки зрения, это приводит к трудностям в выяснении того, является ли деятельность в киберпространстве применением силы, и какова степень ответственности соответствующего государства.

В-пятых, нет юридически значимых глобальных норм для киберпространства. Многие страны проводят собственную политику кибербезопасности, но эти политики, как правило, конкурируют, а не дополняют друг друга.

В-шестых, нет общепринятой интерпретации существующего международного права как *jus ad bellum*, так и *jus in bello*.

III. Решения проблем

С правовой точки зрения, должен быть достигнут консенсус о применимости ПВК в киберпространстве. Работа Группы правительственных экспертов ООН должна быть усилена и по мере целесообразности должно быть заключено юридически обязывающее международное соглашение по кибербезопасности.

Технически, для эффективного противодействия международным кибератакам и укрепления мер доверия, технологически развитые страны, такие как Соединенные Штаты, должны поделиться технологиями атрибуции кибератак. С этой целью следует поощрять совместные исследования и разработку технологий атрибуции.

В целях укрепления сотрудничества и повышения эффективности, необходимо создать международную организацию по кибербезопасности, предпочтительно под эгидой ООН. Её функции могут включать в себя координацию разработки и внедрения соответствующих правовых норм, руководство совместными исследованиями и разработками, обмен кибертехнологиями, и т.д. В процессе выработки норм мы должны продолжить использование опыта и эффективности контактов в формате второй или полуторной «дорожки».

Gao Hui

Cyberinformation Center of China Association for International Friendly Contact (*CAIFC*)

Applicability of the Law of Armed Conflict in Cyberspace

Distinguished Guests!

Ladies and Gentlemen,

It is my privilege to join in your discussion on cyber security at this beautiful Alps town. This year marks the 20th anniversary of China's enter into the internet. The past 20 years witnessed China's rapid development and admirable accomplishment in this field. Up to the end of 2013, China has 0.6 billion netizens, among which half of them has the experience of on-line shopping. Among the top ten international internet companies, three of them are Chinese enterprises. So China has become one of the major powers in cyberspace, and firm guardian for cyber security. Not long ago, Chinese central government established leading group of cyber security and informatization with our President Xi Jinping as group leader. We firmly believe that China needs to join international society in safeguarding cyber security. China Association for International Friendly Contact is committed to friendly communication between China and the rest of the world, we are also one of the founding members for International Information Security Institute. In order to facilitate international cooperation in cyberspace, CAIFC specially established Cyber and Information Center, and invite many Chinese first-class experts on cyber security and related legal specialists as our research fellows. We would love to take this opportunity to intensify cooperation with the representatives and experts of the think tanks present here today.

Now I would love to share some of my thoughts on the applicability of the Law of Armed Conflict in Cyberspace.

The Law of armed conflict (LOAC) usually refers to jus in bello or international humanitarian law. But in the broader sense, it can be used to refer to both *jus in bello* and *jus ad bellum*. This paper uses this concept in the broader sense.

I. Problems with applying LOAC in Cyberspace

Jus ad bellum is generally reflected in articles 2(4) and 51 of the UN Charter. Article 2(4) prohibits the threat or use of force in

international relations, while article 51 allows a state under armed attack to invoke the right of individual or collective self-defense. To note, "use of force" and "armed attack" are two different words. Although there is no definition for the two words in the UN Charter, we can read from the text that only when the use of force reaches the extent of an "armed attack" can the state take measures in self-defense.

Jus in bello is mainly reflected in the Geneva Conventions of 1949 and its additional protocols in 1977, including the basic rules and principles to be observed by the parties during an armed conflict. There are four fundamental principles underlying *jus in bello*, that is to say, military necessity, humanity, distinction and proportionality. The purpose of the principles is to achieve the balance between military necessity and humanity, intending to minimize the suffering caused by armed conflict while not impeding military efficiency.

In my opinion in order to apply LOAC in cyberspace, we need to solve many problems and obstacles. Firstly, as regards *jus ad bellum*, for a cyber operation to constitute a use of force or an armed attack, many problems shall be manifested: what is the right threshold of "use of force" and "armed attack" in cyberspace? When can a right to self-defense be invoked against cyber attack? How can we counter attack for self-defense? How to observe the requirements of "necessary and proportionate" in counterattack? Does a hacker constitute a legitimate target? In fact, although some country argues that a state can invoke the right of self-defense or even preparatory self-defense for imminent cyber threats, the country at the same time points out that "Cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force".

Secondly, as regards *jus in bello*, although customary international law has some limitations on new technologies developed into weapons, it is hard to say that the principles of distinction and proportionality is automatically applicable in cyberspace. Legally, it is subject to further examination and analysis; technically, it has to ensured that cyber attacks are controllable, capable of realizing the requirements of the principles of distinction and proportionality, and capable of accurately assessing possible collateral damage. Problems also arise when other rules of *jus in bello* are applied in cyberspace, such as the law of neutrality.

II. Causes for the problems and obstacles

Firstly, cyberspace is a virtual, interconnected space where it is easy to conceal identity. Cyberspace is thus rather different from the real world. When we are trying to apply the LOAC rules developed for the real world in cyberspace, we have to consider the features of cyberspace.

Secondly, cyber-related concepts are ambiguous and lack common understanding, including cyber war, cyber crime, cyber weapons and cyber security, etc. In this sense, it is quite necessary to define the related terms and concepts.

Thirdly, there is no criterion for assessing the damage caused by cyber attacks. Most commentators use the criterion of "direct physical injury and property damage resulting from the cyber event", but it is not quite clear. Besides, cyber operations feature non-physical damage, which shall also be taken into account. But there is still no consensus on whether non-physical damage can constitute a use of force and how to assess the damage.

Fourthly, it is still difficult to attribute cyber attacks. This is generally a technical issue, including difficulties in ascertaining the sources of attack, the identity and intention of the attacker, the relationship between the attacker and its state. Legally, it results in difficulties in determining whether the cyber activities constitute a use of force, and in determining the responsibility of the relevant state.

Fifthly, there are no valid global cyber norms. Many countries have their own cyber security policy, but the policies are generally competing rather than complementing each other.

Sixthly, there is no generally agreed interpretation of existing international law for both *jus ad bellum* and *jus in bello*.

III. Solutions for the problems

Legally, consensus shall be reached on the applicability of LOAC in cyberspace. The work of UNGGE shall be strengthened and when appropriate a legally binding international cyber security agreement shall be made.

Technically, in order to effectively cope with international cyber attacks and strengthen CBMs, technologically advanced countries such as the United States shall share cyber attack attribution technologies. To this end, joint research and development of attribution-related technologies should be encouraged.

To strengthen cooperation and increase efficiency, it is necessary to establish an international cyber security organization, preferably under the authorization of the UN. Functions may include the coordination of drafting and implementing relevant legal norms, the management of joint research and development and sharing of cyber technologies, etc. We need to further explore the efficiency and wisdom of second track or one and a half track communication in the process of regulation formulation.

И.Н.Дылевский, В.О.Запивахин,
С.А.Комов, А.Н.Петрунин
Министерство обороны Российской Федерации

Об адаптации международно-правового понятия «агрессия» к специфике информационного пространства

Одновременно с развитием информационных технологий появляются тенденции и условия для их использования в агрессивных целях. В последнее время существенно увеличилось количество деструктивных информационных атак, совершаемых с использованием современных информационно-коммуникационных технологий. Их объектами воздействия становятся информационные системы и ресурсы государств (финансов, транспорта, промышленности, масс-медиа, военного назначения и т.п.).

В апреле прошлого года была нарушена работа банковской системы Республики Южная Корея. Кто это сделал и кто за этим стоит теоретически известно, но доказательной базы у южнокорейского руководства нет.

Так называемое хакерское сообщество «Анонимус» регулярно выкладывает в сети «Интернет» различную конфиденциальную информацию, добытую незаконным путем. Что это за организация, кто санкционирует их деятельность (может это спецслужбы конкретного государства), достоверно неизвестно, соответственно непонятно, какие меры противодействия принимать к ним и как квалифицировать их действия.

В марте этого года интернет-ресурсы ведущих российских теле- и радиокомпаний подверглись информационным атакам, целью которых было блокирование их работы. Нашими специалистами отмечается высокопрофессиональное проведение этих воздействий. Чтобы их осуществить, требуется длительная и заблаговременная подготовка. И здесь возникают те же вопросы — кто санкционировал проведение информационных атак на российские интернет-ресурсы, какими силами они осуществлены и как защитить себя в дальнейшем?

Анализ сведений, появляющихся в сети «Интернет» и средствах массовой информации, о подобных деструктивных воздействиях показывает, что в последнее время информационные атаки становятся все сложнее. Прогнозируется, что в ближайшей перспективе объектами их воздействия будут не только

информационные ресурсы в сети «Интернет», но и критически важные объекты инфраструктуры государств, обеспечивающие функционирование промышленности, транспорта, энергетики и другие сферы жизнедеятельности.

Информационные атаки на них могут приводить к серьезным последствиям, вполне сопоставимым с применением традиционных видов оружия. То есть использование информационно-коммуникационных технологий в определенных условиях может стать оружием — «информационным оружием».

В связи с этим возникает вопрос о возможности применения законного права на самооборону в ответ на подобные информационные атаки, которые в данном случае полагается возможным расценивать как акт агрессии.

В рамках третьей профильной группы правительственных экспертов ООН (ГПЭ), закончившей работу в 2013 году, рядом экспертов уже ставился этот вопрос. Но ответа не удалось найти как на этот, так и на другие вопросы, связанные с развитием существующего международного права применительно к специфике информационного пространства. Поэтому в мандат четвертой ГПЭ, которая начнет работу в текущем году, был включен вопрос о том, «как международное право применяется к использованию информационно-коммуникационных технологий государствами»[1].

Такой широкий подход подразумевает в дальнейшем изучение, в том числе, вопроса о возможности применения ст.51 Устава ООН (право на самооборону) к военному реагированию на информационные атаки. А значит и того, что же представляет собой с точки зрения международного права «акт агрессии», совершенный с использованием ИКТ.

Минобороны России, обеспокоенное усилением угрозы появления возможности проведения трансграничных информационных воздействий на информационные системы и ресурсы военного назначения, провело анализ международно-правового понятия «агрессия» в контексте его адаптации к специфике информационного пространства, основные результаты которого изложены в данной статье.

В настоящее время понятие «агрессия» определено Резолюцией Генеральной Ассамблеи ООН 1974 года № 3314 (XXIX). В соответствии со статьей 1 этой резолюции под «агрессией»

[1] «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Резолюция Генеральной Ассамблеи ООН (A/68/37), 18 октября 2013 г.

понимается «*применение вооруженной силы государством против суверенитета, территориальной неприкосновенности или политической независимости другого государства, или каким-либо другим образом, несовместимым с Уставом ООН, как это установлено в настоящем определении*».

Отсюда следует, что понятие «агрессия» не отождествляется с применением вооруженной силы вообще. Для того чтобы признать агрессией какой-либо факт применения вооруженной силы необходимо установить, что вооруженная сила была использована для нарушения государственного суверенитета, территориальной неприкосновенности или политической независимости другого государства.

Нарушение государственного суверенитета, территориальной неприкосновенности или политической независимости другого государства осуществляется в конкретных физических средах (земном, морском и воздушном пространствах). Но существует еще такая сфера, как «информационное пространство»[2], в котором у каждого государства существуют свои интересы, и их также необходимо защищать. В отличие от физических сред оно не имеет явно выраженных государственных границ. Не случайно его называют «глобальным» и «трансграничным», то есть выходящим за границы государства.

Вместе с тем, в последнее время мировое экспертное сообщество постепенно приходит к пониманию того, что понятие «государственный суверенитет» имеет такое же прямое отношение к информационному пространству, как и к геофизическим видам пространства. Все информационно-коммуникационные технологии (средства, системы), используемые для формирования информационного пространства, имеют своих национальных владельцев и размещены в пределах суверенных границ конкретных государств. Поэтому трансграничное нарушение их нормального функционирования (уничтожение, вывод из строя, подавление), которое может осуществляться с использованием вооруженной силы, основанной на использовании традиционного оружия, может ква-

---

[2] «Информационное пространство» — сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию (см. «Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности», вступившее в силу 2 июня 2011 года).

лифицироваться как нарушение суверенитета, территориальной неприкосновенности или политической независимости другого государства, т.е. как агрессия.

Возьмем условную гидроэлектростанцию. Нет сомнений, она является критически важным объектом инфраструктуры государства. Если кто-то нанесет по такой станции удар любым из имеющихся современных вооружений, то это приведет к колоссальным разрушениям и гибели людей. Это будет считаться актом агрессии. А если, использовав информационно-коммуникационные технологии, нарушена работа автоматизированной системы управления этой станции, и это привело к ее разрушению и гибели людей? Это будет актом агрессии? Да, здесь тоже имеет место быть агрессия.

Вместе с тем, еще не сложилась практика применения «информационного оружия»[3] против таких объектов, результаты которого были бы соизмеримы с ущербом от традиционных видов оружия. Однако, по мнению ряда экспертов, уже есть примеры, подтверждающие наличие у отдельных информационно-коммуникационных технологий (ИКТ) таких трансграничных возможностей, которые позволяют квалифицировать их реализацию как акт вооруженной агрессии. Например, компьютерные атаки с использованием программного вируса Stuxnet на иранские ядерные объекты. Они вполне могут претендовать на первое место в номинации «агрессия в киберпространстве» по итогам 2010 года[4]. Два других примера компьютерных атак, хотя и отличаются методами и средствами и объектами воздействия, также могут рассматриваться в качестве актов агрессии. Речь идет о DDOS-атаках на информационную инфраструктуру Эстонии в апреле-мае 2007 года и Грузии в августе 2008 года. Они надолго парализовали работу систем государственного управления и обеспечения жизнедеятельности в этих странах.

Что это, как не нарушение государственного суверенитета, территориальной неприкосновенности или политической независимости другого государства? Неслучайно эстонское руководство, всерьез обеспокоенное уязвимостью своей ин-

---

[3] «Информационное оружие» — информационные технологии, средства и методы, применяемые в целях ведения информационной войны (см. «Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности», вступившее в силу 2 июня 2011 года).

[4] Виктор Мясников Десять главных военных событий 2010 года, НВО, 24.12.2010; Top Military Developments of 2010, StrategyPage, January 14, 2011.

формационной инфраструктуры, добилось распространения ст. 5 Вашингтонского договора (коллективный ответ на вооруженное нападение) на подобного рода компьютерные атаки и развернуло в Таллине натовский центр кибероборонны, призванный осуществлять симметричный ответ на них.

Вместе с тем практическое признание трансграничных компьютерных атак актами агрессии пока проблематично.

Во-первых, не разработаны методы и средства оперативного и точного определения местоположения и национальной принадлежности источников информационных атак.

Во-вторых, даже если эти источники идентифицированы, то возникает проблемный вопрос — как установить связь некоего сетевого сообщества с заинтересованными государственными структурами? Что если его члены действуют исключительно из патриотических или иных побуждений? Кто должен нести международную ответственность за результаты осуществления вредоносной компьютерной атаки? Как безошибочно установить наличие акта агрессии? Законны ли в принципе ответные действия на такие компьютерные атаки в рамках реализации права на самооборону в соответствии со ст. 51 Устава ООН? И против кого конкретно они должны осуществляться?

Поиском ответов на эти вопросы сейчас активно занимаются различные страны. Отдельными его группами уже предлагаются возможные «ответы». В частности, в экспертном сообществе США преобладает мнение, что признак государственной принадлежности источника информационной атаки в ходе ее квалификации вообще не является существенным. При этом они опираются на т.н. концепцию «ответственного поведения» государств. По мнению американцев, такое поведение означает, что национальные правительства должны нести ответственность за любые компьютерные атаки, осуществляемые с территории их государства, не зависимо от их мотивации и политико-правового статуса заказчика и исполнителя.

По нашему мнению, подобный подход к квалификации агрессивных актов неприемлем.

Войны развязывают государства и ведут с использованием вооруженных сил. Что касается иных физических и юридических лиц, то они могут считаться источником агрессии лишь в том случае, если действуют по заказу государственных структур. Данное положение закреплено в статье 3 Резолюции № 3314 и будет более подробно проанализировано ниже.

Вместе с тем, лица, которые осуществляют трансграничные нападения, руководствуясь террористическими, экстремистскими или корыстными мотивами, не могут рассматриваться в качестве источника агрессии. В этом случае информационные атаки должны квалифицироваться как террористические уголовные преступления. Эти преступления имеют антиобщественный характер и поэтому различные государства, как правило, осуществляют совместное уголовное преследование виновных лиц в рамках международной правовой помощи.

Государства, с территории которых осуществляются трансграничные преступления, должны также нести за них международную ответственность, так как они обязаны обеспечивать правопорядок на своей территории. Однако эта ответственность не имеет отношения к агрессии, которое по своей природе связано с военной политикой государства и ее прямой или косвенной реализацией в незаконной военной деятельности.

В статье 2 Резолюции № 3314 указывается, что «*применение вооруженной силы государством первым в нарушение Устава является свидетельством акта агрессии, хотя Совет Безопасности может в соответствии с Уставом сделать вывод, что определение о том, что акт агрессии был совершен, не будет оправданным в свете других соответствующих обстоятельств, включая тот факт, что соответствующие акты или их последствия не носят достаточно серьезного характера*».

При проведении международно-правовой квалификации какого-либо конкретного акта трансграничного военного применения информационно-коммуникационных технологий данное положение следует трактовать с учетом двух основных факторов.

Во-первых, агрессором может быть признано то государство, которое первым провело информационную атаку на другое государство для решения своих военно-политических задач. Этот временной фактор в соответствии с резолюцией свидетельствует в пользу признания акта агрессии.

Во-вторых, для вынесения окончательного вердикта о том, является ли данная информационная атака актом агрессии или нет, Совет Безопасности ООН должен оценить характер последствий этой атаки. В том случае, если последствия будут признаны серьезными, атака может быть квалифицирована как акт агрессии.

Могут ли быть признаны серьезными упоминавшиеся ранее компьютерные атаки на иранские ядерные объекты, если,

по оценкам специалистов, в итоге их проведения ядерная программа Тегерана была отброшена на два года назад[5]. Если это так, то теоретически Иран может быть признан Советом Безопасности ООН объектом агрессии, а авторы и исполнители компьютерных атак, если они действовали по государственному заказу, — агрессорами.

Однако на практике принять такое решение сейчас вряд ли удастся, т.к. для определения серьезности военного применения ИКТ Совету Безопасности ООН необходим соответствующий критериальный аппарат. В настоящее время роль такого аппарата в отношении применения традиционной вооруженной силы выполняет перечень возможных актов агрессии, приведенный в ст. 3 резолюции.

Во-первых, наиболее просто вопрос такой квалификации может быть решен с использованием критерия «*нападение вооруженными силами государства на сухопутные, морские или воздушные силы, или морские и воздушные флоты другого государства*» (п. d). При этом по смыслу этого положения не имеет принципиального значения вид применяемого оружия. Поэтому проведение вооруженными силами одного государства информационных атак на информационную инфраструктуру вооруженных сил другого государства может быть признано Советом Безопасности ООН актом агрессии.

Во-вторых, для квалификации агрессии с использованием ИКТ могут быть использованы такие критерии, как «*нападение вооруженных сил государства на территорию другого государства*» (*п. a*) *и «применение любого оружия государством против территории другого государства*» (п. b). В этом случае применение «информационного оружия» специальными подразделениями армии, флота и авиации может быть определено как нападение вооруженных сил на территорию другого государства.

В состав территории государства входят: сухопутная территория, акватория, воздушное пространство[6]. Что касается «информационного пространства», то вопрос о его включении в содержание понятия «территория государства» пока не только не решен, но даже еще и не рассматривался в такой постановке. Вместе с тем, как уже говорилось, именно на тер-

---

[5] Барынькин В.М. Минное поле информационных войн. Военно-промышленный курьер, №14, 10 апреля 2013 г., с. 6–7.

[6] Бабурин С.Н. Территория государства: Правовые и геополитические проблемы. М.: Из-во Московского государственного университета, 1997.

ритории страны размещены «информационные ресурсы»[7], формирующие национальный сегмент информационного пространства. Поэтому далее под «нападением вооруженных сил государства на территорию другого государства» вполне допустимо понимать в том числе «применение вооруженными силами государства информационного оружия против информационных ресурсов другого государства».

Особый интерес для возможной квалификации агрессии с использованием ИКТ представляет критерий «*действие государства, позволяющего, чтобы его территория, которую оно предоставило в распоряжение другого государства, использовалась этим другим государством для совершения акта агрессии против третьего государства*» (п. f). Под действие данного критерия, в случае распространения его на информационное пространство, могут попасть все государства, на территории которых расположены прокси-серверы, используемые государствами-агрессорами для проведения анонимных компьютерных атак.

И наконец, применение критерия «*засылка государством или от имени государства вооруженных банд, групп, иррегулярных сил или наемников, которые осуществляют акты применения вооруженной силы против другого государства, носящие столь серьезный характер, что это равносильно перечисленным выше актам, или его значительное участие в них*» (п. g). Его использование возможно в том случае, если агрессивные компьютерные атаки осуществляются не подразделениями регулярных вооруженных сил, а иными силами и средствами, выполняющими задачи в их интересах и от их имени.

Следует отметить, что резолюция № 3314 дает Совету Безопасности возможность не ограничиваться приведенным перечнем. В ее ст. 4 указывается, что «*вышеприведенный перечень актов не является исчерпывающим, и Совет Безопасности может определить, что другие акты представляют собой агрессию согласно положениям Устава*». Поэтому конкретные критерии квалификации агрессии с использованием ИКТ могут быть дополнительно сформулированы в явном виде. Например, таким критерием может быть «применение вооружен-

[7] «Информационные ресурсы» — информационная инфраструктура, а также собственно информация и ее потоки (см. «Соглашение между правительствами государств–членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности», вступившее в силу 2 июня 2011 года).

ными силами государства информационного оружия против критически важных объектов другого государства».

Представляется также необходимым сформулировать критерий информационного нападения с применением современных информационно-коммуникационных технологий (социальные сети, мобильная радиосвязь и др.), получившего широкое распространение в последнее время. Таким критерием может стать «пропаганда государством войны и применения силы, распространение подстрекательской информации, способствующие дестабилизации внутригосударственной и международной обстановки, развязыванию и эскалации вооруженных конфликтов».

В том случае, если эти деяния будут признаны применением вооруженной силы государством или группой государств против суверенитета, территориальной неприкосновенности или политической независимости другого государства, они должны квалифицироваться в качестве актов агрессии. Это закономерно влечет за собой ответственность, как государств, так и физических лиц, причастных к их подготовке и проведению.

Устав ООН, закрепляя принцип невмешательства в дела, входящие во внутреннюю компетенцию любого государства, делает из этого принципа исключение только в случае применения принудительных мер на основании главы VII, то есть по решению Совета Безопасности ООН, а не по собственному усмотрению какого-либо государства, либо коалиции государств.

Для дальнейшего исследования возможных подходов к выявлению информационных аспектов агрессии интерес представляет вопрос разграничения понятия «агрессия» и «самооборона», право на которую закреплено ст. 51 Устава ООН, где записано: «*Настоящий Устав ни в коей мере не затрагивает неотъемлемого права на индивидуальную или коллективную самооборону, если произойдет вооруженное нападение на Члена Организации, до тех пор, пока Совет Безопасности не примет мер, необходимых для поддержания международного мира и безопасности. Меры, принятые Членами Организации при осуществлении этого права на самооборону, должны быть немедленно сообщены Совету Безопасности и никоим образом не должны затрагивать полномочий и ответственности Совета Безопасности, в соответствии с настоящим Уставом, в отношении предпринятия в любое время таких действий, какие он*

сочтет необходимыми для поддержания международного мира и безопасности».

Характерно, что данное положение трактуется различными специалистами международного права по-разному.

В частности, российская юридическая наука утверждает, что вооруженное нападение является первичным по отношению к самообороне. Поэтому основанием для нее может быть только реальное вооруженное нападение, а не его угроза, поскольку в последнем случае самооборона утрачивает свое ответное качество, и сама превращается в вооруженное нападение.

Западные эксперты напротив считают, что государство имеет право прибегнуть к самообороне превентивно, т.е. не только в случае вооруженного нападения на него, но и в случаях его угрозы, а также для защиты своих экономических интересов и граждан, которые подвергаются опасности при их нахождении на территории других государств. В ходе первой Конференции по обзору Римского статута Международного уголовного суда (МУС) практически единодушно отвергнуто предложение делегации США об исключении юрисдикции МУС в случае, когда государство-агрессор действовало «*добросовестно и с целью предупреждения преступлений, предусмотренных статьями 6, 7 и 8 Статута*»[8]. То есть попытка США оградить себя от ответственности в случае проведения очередной т.н. «гуманитарной интервенции» не нашла поддержки более 100 государств-членов МУС.

По смыслу ст. 51 Устава ООН возможность обращения к силе в порядке самообороны, к примеру, от компьютерных трансграничных атак допустима только в случае, если они будут признаны Советом Безопасности ООН актом вооруженного нападения. Поэтому превентивное и расширенное толкование самообороны от таких атак, применяемое сейчас в руководящих документах США и НАТО, противоречит современному пониманию права государства на принудительное обеспечение своей территориальной неприкосновенности и политической независимости от насильственного акта в форме вооруженного нападения.

Таким образом, анализ информационных аспектов «определения агрессии» свидетельствует о необходимо-

---

[8] Богуш Г. Обзорная конференция по Римскому статуту: новые горизонты международного уголовного правосудия. Сравнительное конституционное обозрение, № 5 (78). 2010, с. 1–9.

сти его адаптации для применимости к информационно-коммуникационным технологиям на основе использования уже существующих положений Резолюции № 3314, о которых говорилось выше. И включения в статью 3 этой Резолюции дополнительных определений возможных актов агрессии в информационном пространстве.

В частности, к ним, например, могут быть отнесены:

- **применение вооруженными силами государства информационного оружия против критически важных объектов другого государства, в результате которого возникли техногенные катастрофы**;
- **государственная пропаганда, трансграничное распространение которой привело к дестабилизации внутригосударственной и международной обстановки, развязыванию и эскалации вооруженных конфликтов**.

В заключение необходимо отметить, что деятельность по выработке юридически обязательного «определения агрессии», длящуюся уже более 60 лет, нельзя считать завершенной, так как данное определение не обладает необходимой юридической силой. Это связано с тем, что Генеральная Ассамблея ООН, чьей резолюцией было закреплено определение агрессии, не уполномочена принимать решения, обязательные для исполнения всеми государствами-членами Организации. Однако в обозримой перспективе эта проблема может быть решена. В частности, в 1998 году МУС была предоставлена юрисдикция в отношении «преступления агрессии» при условии, что она начнет осуществляться после того как будет принято определение этого преступления. В последующие годы понятие «преступление агрессии» было сформулировано Специальной рабочей группой путем инкорпорации в Римский Статут «Определения агрессии», которое прилагалось к Резолюции Генеральной Ассамблеи ООН 3314 (XXIX) 1974 года. На первой Конференция по обзору Римского статута МУС в июне 2011 года была принята резолюцию, согласно которой в него включаются определение «преступление агрессии» и условия, при которых Суд может осуществлять юрисдикцию в отношении этого преступления[9]. Фактическое осуществление юрисдикции зависит от решения, которое будет принято на очередной обзорной конференции после 1 января 2017 года. Таким образом, ожидаемое включение определения агрессии

[9] Конференция по обзору Римского статута Международного уголовного суда. Кампала, 31 мая — 11 июня 2010, года. Официальные отчеты.

в Римский статут, придаст ему необходимую юридическую силу.

Что касается информационных аспектов этого международно-правового понятия, то их учет в общем «определении агрессии» потребует инициирования отдельных переговорных процессов, как в рамках ООН, так и в структурах МУС. Лишь в итоге их проведения и консенсусного завершения мировое сообщество сможет получить универсальную международно-правовую методологию отнесения конкретных фактов трансграничного применения современных ИКТ к актам вооруженной агрессии.

I.N.Dylevskiy, V.O.Zapivakhin,
S.A.Komov, A.N.Petrunin
Ministry of Defense of the Russian Federation

Adaptation of international legal concept of "aggression" to the specifics of information space

With the development of information technologies, there emerge trends and conditions for their use for aggressive purposes. Recently there was a significant increase in number of destructive information attacks by means of contemporary information and communication technologies. They target information systems and information resources of States (*financial, transportation, industrial, media, military, etc.*).

Last year in April the banking system of the Republic of South Korea was disrupted. In theory it is known who did this and who is behind this, but the South Korean leadership does not have the evidentiary foundation.

The so-called "Anonymous" hacker community regularly puts various illegally obtained confidential information on the Internet. What kind of organization this is, who authorizes its activities (*perhaps the secret services of a particular State*) *is not known for sure, and thus it is not at all clear what countermeasures should be taken against them and how to qualify their actions.*

This year in March, online resources of major Russian TV and radio companies suffered information attacks, aimed to obstruct their work. Our experts have noted a highly professional conduct of these attacks. Their implementation requires a lengthy preliminary preparation. And here the same questions arise — who authorized information attacks on Russian Internet resources, what forces carried them out and how to protect oneself in the future?

Analysis of information about such destructive effects, found on the Internet and in the media, shows that lately information attacks are becoming more complex. It is predicted that in the near future they will target not only information resources on the Internet, but also the national critical infrastructure, which supports operation of industry, transportation, energy and other spheres of life.

Information attacks on critical infrastructure can lead to serious consequences, comparable with the use of conventional weapons. That is, the use of information and communication technologies in certain conditions can become a weapon — an "Information weapon".

In this regard, the question arises about the possibility to invoke a legitimate right to self-defense in response to such information attacks, which in this case, as it appears, is possible to qualify as an act of aggression.

This question has already been raised by a number of experts within the framework of the third UN Group of Governmental Experts (GGE) (concluded its work in 2013). But one couldn't find answers to this and other questions related to the development of existing international law in relation to the specifics of the information space. Therefore, the fourth mandate of GGE (which will start this year) includes a question "how International Law is applied to the use of Information and Communication Technologies by countries."[1]

This broad approach implies among other things the study of applicability of Article 51 of the UN Charter (the right to self-defense) to military response to information attacks. And therefore the study of what comprises an act of aggression with the use of ICT from the standpoint of International Law.

Russian Ministry of Defense is also concerned about the increasing threat of such comparable to known acts of aggression cross-border information effects on military information systems and resources. In this regard, the Russian military experts have analyzed the international legal concept of "aggression" in the context of its adaptation to the specifics of information space, the main results of analysis are described in this article.

Aggression is currently defined by UN General Assembly Resolution 3314 (XXIX) of 1974[2]. According to the Article 1 of this Resolution, aggression is "the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations, as set out in this Definition".

It follows that the concept of "aggression" is not identified with the use of force of arms in general. In order to recognize any fact of force of arms use as aggression, it is necessary to establish that force of arms was used to breach sovereignty, territorial integrity or political independence of another state.

Violation of sovereignty, territorial integrity or political independence of another state is carried out in specific physical environments (land, sea and airspace). But there also exists "Informa-

[1] UN General Assembly Resolution 68/243. Developments in the field of information and telecommunications in the context of international security

[2] "Definition of Aggression" UN General Assembly Resolution 3314 (XXIX), 1974

tion Space"[3], where each State has its interests, which must be protected. In contrast to physical environment, it has no distinct state borders. It stands for reason that it is often called "global" and "cross-border", that is they cross national borders.

However, currently the global expert community is gradually developing an understanding that the concept of "state sovereignty" has the same direct relation to information space, as to other forms of geophysical space. All information and communication technologies (assets, systems), used to form the information space, have their national owners and are housed within the sovereign borders of individual States. Therefore, cross-border violations of their normal functioning (destruction, incapacitation, suppression), which can be accomplished by force of arms based on the use of traditional weapons, could qualify as a violation of the sovereignty, territorial integrity or political independence of another state, i.e. as an aggression.

Let's take conditional hydroelectric power plant. It is no doubt a critical infrastructure of the State. If someone attacks it by means of any of the available modern weapons, it will lead to immense destruction and loss of life. This would be considered an act of aggression. And if, the automated control system of the station is disrupted by means of information and communication technologies, and this led to its destruction and loss of life? Would it be an act of aggression? Yes, here as well, there happens to be an act of aggression.

Having said that, the practice of "information weapons"[4] use against such targets, the results of which would be commensurate with the damage caused by conventional weapons has not yet developed. However, according to some experts, there are already examples confirming that certain information and communication technologies (ICT) have such cross-border capabilities that allow one to qualify their use as an act of armed aggression. For example, computer attack using the Stuxnet virus on Iran's nuclear facilities

---

[3] "Information space" — field of activities related to generating, transforming, transferring, using and storing information which influences, in particular, individual and public mind, information infrastructure and information as such (see Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, 2 June 2011)

[4] "Information weapon" — information technologies, ways and means of waging an information war. (see Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, 2 June 2011)

may well claim the first place in the 2010 nomination "aggression in cyberspace"[5]. Two other examples of cyberattacks, although used different methods, tools and targets, can also be considered as acts of aggression. These examples are DDOS-attacks on the information infrastructure of Estonia in April — May 2007 and Georgia in August 2008. They permanently paralyzed public administration and municipal maintenance systems in these countries.

What is this but a violation of state sovereignty, territorial integrity or political independence of another country? No wonder that Estonian government, being seriously concerned about vulnerabilities of their information infrastructure, got Article 5 of the Washington Treaty (collective response to an armed attack) to extend to this kind of computer attacks and deployed NATO Cooperative Cyber Defense Centre of Excellence in Tallinn, to carry out a symmetrical response to them.

However, the practical recognition of cross-border cyber attacks as acts of aggression is significantly complicated.

Firstly, there are no developed methods and tools for rapid and precise identification of location and national identity of source of cyberattacks.

Secondly, even if the sources of malicious activity are identified, how to expose a connection between a certain network community with government stakeholders? What if its members act solely out of patriotism or other motives? Who should bear international responsibility for the outcome of a malicious cyberattack? How can one accurately establish the presence of an act of aggression in this case? Is a response to such computer attacks legitimate in principle as part of the right to self-defense under Article 51 of the UN Charter? And at whom exactly should this response be directed?

Countries are actively looking for answers to these questions. Certain groups of experts within these countries have already come up with possible "answers". In particular, among the U.S. expert community the dominant opinion is that the national identity of information attack is not at all essential in the course of its qualifications. At the same time they rely on the so-called concept of "responsible behavior" of countries. From American perspective this behavior implicates that national governments should be responsible for any computer attacks carried out from their territory, regardless of motivation of attack and political and legal status of contractor and perpetrator.

---

[5] V.Miasnikov, Top Military Developments of 2010, StrategyPage, January 14, 2011.

In our opinion, such an approach to qualification of aggressive acts is unacceptable.

Wars are unleashed and waged by countries with the use of armed forces. As for individuals and legal entities, they can be considered a source of aggression only if they act on order by governmental authorities. This provision is formalized in Article 3 of Resolution 3314 and will be further analyzed hereafter.

Having said that, Individuals who carry out cross-border attacks with terrorist, extremist or interested motives, cannot be considered a source of aggression. In this case, information attacks should be classified as terrorist, extremist or other criminal offenses. These crimes are antisocial in nature and therefore different countries as a rule cooperate on criminal prosecution of those responsible within the framework of international legal assistance.

Countries must be internationally liable for transboundary crimes carried out from their territory, since they are under obligation to administer the law on their territory. However, this responsibility is not related to the crime of aggression, which by its nature is associated with national military policy and its direct or indirect implementation in the form of illegal military activities.

Article 2 of Resolution 3314 states that *"the first use of armed force by the State in contravention of the Charter shall constitute prima facie evidence of an act of aggression although the Security Council may, in conformity with the Charter, conclude that a determination that an act of aggression has been committed would not be justified in the light of other relevant circumstances, including the fact that the acts considered or their consequences are not of sufficient gravity".*

In the course of international-legal qualification of specific act of cross-border military use of ICT this provision should be interpreted with regard to two principal facilitations.

Firstly, a country which first executed an information attack on another state to accomplish its military and political objectives may be recognized as aggressor. This time factor, in accordance with the resolution favors the recognition of an act of aggression.

Secondly, to take the final verdict on whether or not this information attack is an act of aggression, the UN Security Council must assess the nature of consequences of this attack. In case the effects are found to be of sufficient gravity, the attack can be qualified as an act of aggression.

Can the aforementioned cyberattacks on Iranian nuclear facilities be considered of sufficient gravity if, according to experts, as a result of these attacks, Tehran's nuclear program was set back

two years?[6] If so, then theoretically Iran could be recognized by the Security Council of the UN as a target of aggression, and the authors and perpetrators of computer attacks, if they acted on government orders — as aggressors.

However, presently this decision is unlikely to be made in practice, as the UN Security Council needs corresponding criterial framework to determine the gravity of the military use of ICT. Currently a list of possible acts of aggression in Article 3 of Resolution 3314 serves as similar framework regarding the use of conventional armed force:

Firstly, the issue of such qualification can be easily resolved by using the criterion of "*an attack by the armed forces of a State on the land, sea or air forces, or marine and air fleets of another State*" (pt.d). At the same time, in the context of this provision, it does not matter what kind of weapons are used. Therefore, cyberattacks launched by armed forces of one country against information infrastructure of the armed forces of another country may be recognized by the Security Council as an act of aggression.

Secondly, for qualification of aggression by means of ICTs one can use the criteria *"attack by the armed forces of a State on the territory of another State"* (*pt.a*) *and "use of any weapons by a State against the territory of another State"* (*pt.b*). In this case, the use of information weapons by Special Forces of army, navy and air force can be qualified as an attack by the armed forces on the territory of another State.

The territory of a State includes land, water, aerial domains[7]. As for the "information space", not only the question of its inclusion in the concept of "territory of a State" has not been resolved, but it has not even been considered from this standpoint. However, it is obvious that "information resources"[8] which form the national segment of the information space are precisely on the territory of a State. Therefore, further by "attack by the armed forces of a State on the territory of another State" we will mean among other things "the use of armed forces of a State information weapon against information resources of another state".

---

[6] V.Barinkin "Minefield of information wars" Military-industrial courier №14, April 10, 2013, p. 6–7.

[7] S.Baburin "Territory of the state. Political and geopolitical issues", Published in Moscow State University 1997.

[8] "Information resources" — information infrastructure, as well as information as such and its flows (see Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, 2 June 2011)

Criterion *"the action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State"* (pt.f) is of special interest for possible qualification of aggression using ICT. The scope of this criterion in case it extends to information space, can encompass all States which have on their territory proxy servers that are used by aggressor States for anonymous cyberattacks.

And finally, the use of the criterion *"the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein"* (pt.g). It can be relevant if aggressive computer attacks are carried out not by units of the regular armed forces but by other forces and means executing tasks in their interest and on their behalf.

It should be noted that the Resolution 3314 doesn't limit the Security Council to the list noted above. Article 4 states that *"the acts enumerated above are not exhaustive and the Security Council may determine that other acts constitute aggression under the provisions of the Charter"*. Therefore, the specific qualification criteria of aggression with the use of ICT can be further explicitly defined. For example, "the use of information weapons by armed forces of a State against objects of critical infrastructure of another State" may be such a criterion.

It seems essential to formulate a criterion for recently proliferated information attacks that use modern information and communication technologies (social networks, mobile communications, etc.). "State-sponsored propaganda of war and use of force, dissemination of inflammatory information aimed on destabilization of national and international situation, outbreak and escalation of armed conflict" can be such a criterion.

In case these actions are recognized as the use of armed force by State or group of States against sovereignty, territorial integrity or political independence of another State, they should be qualified as acts of aggression. This naturally entails responsibility for nations and individuals involved in their preparation and execution.

UN Charter enshrines the principle of non-interference in matters within the domestic jurisdiction of any State, and makes an exception to this principle only in case of enforcement measures under Chapter VII, that is by descision of the UN Security Council, and not at the sole discretion of any State or coalition of states.

To further investigate the possible approaches to identification of the information aspects of aggression; of particular interest is

the question of distinction of concepts "aggression" and "self-defense", as enshrined in Article 51 of the UN Charter: "*Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security".*

It is indicative that this provision is interpreted by different international law specialists in different ways.

In particular, Russian science of law states that an armed attack is primary in relation to self-defense. Therefore, only a real armed attack, rather than the threat of it, can be the basis for self-defense, as otherwise it loses its self-defense response quality, and itself turns into an armed attack.

Western experts, in contrast, believe that the state has the right to resort to self-defense preemptively, not only in case of an armed attack, but also in case of a threat, or to protect economic interests and citizens who are at risk in other countries. In the course of the first Review Conference of the Rome Statute of the International Criminal Court (ICC), the proposal made by the United States to exclude the jurisdiction of the ICC when the aggressor state acted in *"good faith and to prevent crimes envisaged in Articles 6, 7 and 8 of the Statute*"[9] was almost unanimously rejected. Thus, the U.S. attempt to shield themselves from liability in the event of another so-called "humanitarian intervention" was not supported by more than 100 member states of the ICC.

By implication of Article 51 of the UN Charter, the recourse to force in self-defense, for example, in the event of cross-border computer attacks, is allowed only if they are recognized by the Security Council as an act of armed attack. Therefore, preempive and extended interpretation of self-defense against such attacks given in guideline documents of the U.S. and NATO, contradicts the current understanding of the right of the State to ensure its territorial integrity and political independence from the act of violence in the form of an armed attack.

---

[9] G.Bogush Review Conference of the Rome Statute: new horizons of international criminal justice. Comparative constitution review № 5 (78)2010, pp.1-9

Thus, analysis of information aspects of "definition of aggression" testifies the need of its adaptation to be applicable to information and communication technologies on the basis of the aforementioned existing provisions of Resolution 3314. And inclusion of the possible acts of aggression in the information space in Article 3 of this Resolution.

In particular, it is proposed to include:

the use of information weapons by armed forces of a State against critical infrastructure of another State;

State propaganda of war and use of force, dissemination of inflammatory information to promote destabilization of national and international situation, outbreak and escalation of an armed conflict.

In conclusion, it should be noted that the work on the elaboration of a legally binding "Definition of Aggression", that has been going on for more than 60 years, cannot be considered finished, since this definition lacks the necessary legal power. This is due to the fact that the UN General Assembly, whose resolution codified the definition of aggression, is not empowered to make decisions binding on all Member States of the Organization. However, in the foreseeable future, this problem can be solved. In particular, in 1998, the ICC was given jurisdiction over the "crime of aggression", provided that it will be implemented after the definition of this crime will be accepted. In subsequent years, the concept of "crime of aggression" was conceived by Special Working Group by legislative restatement in the Rome Statute of "Definition of Aggression", annexed to the UN General Assembly Resolution 3314 (XXIX) of 1974. During the first Review Conference of the Rome Statute of the ICC in June 2010, there was adopted a Resolution, according to which the Rome Statute includes the definition of "crime of aggression" and conditions under which the Court may exercise jurisdiction over this crime[10]. The actual exercise of jurisdiction depends on decisions to be taken at the next Review Conference after January 1, 2017 . Thus, the expected inclusion of a definition of aggression in the Rome Statute will provide it with necessary legal force.

As for information aspects of this international legal concept, their regard in the general "definition of aggression" would require

[10] Review Conference of the Rome Statute of the International Criminal Court, Campala, May 31 — June 11, 2010, Official proceedings

the initiation of separate negotiation processes, both within the UN and in the structures of the ICC. Only as a result of this negotiation processes and their completion with a consensus can the world community receive a universal international-legal methodology for classification of specific facts of cross-border use of modern ICTs as acts of armed aggression.

Н.В.Соколова

Министерство иностранных дел Российской Федерации

О международно-правовых аспектах использования информационно-коммуникационных технологий: опыт Группы правительственных экспертов ООН по международной информационной безопасности

Уважаемые дамы и господа, коллеги!

Хочу поблагодарить организаторов сегодняшней встречи за возможность обсудить в кругу экспертов такую актуальную и приоритетную проблематику как международно-правовые аспекты использования информационно-коммуникационных технологий (ИКТ).

Скажу прямо: для политиков и дипломатов эта тема — во многом «терра инкогнита». ИКТ, как полувеком ранее атомные технологии, открыли новую эпоху в истории человечества. Теперь нам предстоит определить на международном уровне «правила игры» в информационном пространстве, что не было вовремя сделано применительно к ядерной сфере. Как известно, результатом стала гонка вооружений, ограничение которой потребовало колоссальных усилий со стороны международного сообщества.

От результатов сегодняшней дискуссии зависит, будет ли «игра» в информационном пространстве честной.

Актуальность такого разговора невозможно переоценить. Если прежде угрозы в информационной сфере казались хотя и пугающей, но отдаленной перспективой, то сейчас стало очевидно: время «преамбул» прошло. Пора переходить к конкретным решениям.

Всеобщее признание этого факта иллюстрирует, например, то, что в ООН международная информационная безопасность (МИБ) превратилась в полноценный, влиятельный трек, наряду с разоружением и другими «классическими» темами. В прошлом году беспрецедентное количество стран (более 40) поддержало резолюцию Генассамблеи ООН о создании новой Группы правительственных экспертов (ГПЭ) по МИБ. Несмотря на бюджетные проблемы, с которыми в настоящее время сталкивается ООН, финансирование на этом направлении не только не пострадало, но и увеличено: ГПЭ в рас-

ширенном составе проведет четыре (а не три, как это было раньше) заседания. Первое из них состоится уже в июле в Нью-Йорке.

Позвольте мне использовать нашу встречу в Гармише, эту уникальную возможность напрямую обратиться к экспертам, и очертить те «проблемные узлы», распутывать которые нам придется в ходе работы ГПЭ. В первую очередь, это вопросы международно-правового регулирования информационной сферы.

Как оказалось, на этой дороге легко заблудиться. Вот и наш сегодняшний разговор до этой минуты был целиком сфокусирован на обсуждении одного документа — «Таллиннского руководства по применению международного права к ведению кибервойны». Складывается впечатление, что это единственная наработка в этой сфере, у которой нет альтернатив. Принципиальное несогласие вызывает сама постановка задачи — в основе доклада лежит тезис о неизбежности конфликтов в сфере использования ИКТ, при этом как данность преподносится невозможность их предотвращения. Весь последующий анализ строится на основе именно этих предпосылок.

В связи с этим возникает вопрос: какой смысл тогда вообще вести затратные международные дискуссии, если мы заранее расписываемся в собственном бессилии и неспособности предотвратить войну в информационном пространстве?

С другой стороны, не слишком ли много внимания уделяется докладу экспертного уровня, если даже сами авторы оценивают его выводы как устаревшие?

В вопросе о международно-правовом регулировании использования ИКТ мы начинаем далеко не «с нуля» и не «от Таллинна». В то время как отдельные страны увлеченно разрабатывали «правила ведения войны» в информационном пространстве, Россия выступила с правилами ее предотвращения.

В 2011 г совместно с партнерами по ШОС мы распространили проект «Правил поведения в области обеспечения МИБ». В его основе — идея предотвращения, в противовес легализации, конфликтов в сфере использования ИКТ. «Правила» по своему духу являются «джентльменским соглашением» стран, которые, руководствуясь здравым смыслом, а не идеологическими установками, стремятся гарантировать мир в информационном пространстве.

Отклики со стороны других государств продолжают поступать. Вдохновляет то, что с течением времени интерес к документу на политических площадках возрастает.

Не скрою, в адрес «Правил» звучат и критические оценки, хотя конкретного обоснования, почему документ не может стать международно- правовой основой регулирования поведения государств в сфере ИКТ, до сих не смог представить никто. Складывается впечатление, что зачастую критика связана не столько с его содержанием, сколько с «аллергией» на инициативу, как исходящую от стран ШОС.

Вызывает удивление в связи с этим молчание экспертного сообщества, которое кажется настолько увлеченным «Таллиннским руководством», что — то ли по инерции, то ли умышленно — игнорирует альтернативные инициативы. Еще больше разочаровывают оценки в духе «не читал, но осуждаю». Хотя именно реальные и научно обоснованные замечания экспертов могли бы помочь доработать «Правила поведения» в конструктивном ключе.

Теперь о позитивном.

Нам уже о многом удалось договориться на самом высоком международном уровне. В июне прошлого года завершила работу предыдущая ГПЭ ООН по МИБ. Дебаты были острыми и велись до последнего момента. Но они показали, что перед лицом общих угроз консенсус возможен даже в том случае, если между участниками есть разногласия по отдельным вопросам. В итоге был принят доклад, который однозначно закрепил, что все страны заинтересованы в развитии ИКТ в мирных целях, в также в предотвращении конфликтов, вызванных их применением.

«Точкой отсчета» для нашего разговора в дальнейшем, по общему мнение экспертов ГПЭ, должна стать нацеленность на предотвращение конфронтации с применением ИКТ. Это особенно важно теперь, когда на повестку дня фактически выносятся вопросы войны и мира в информационном пространстве.

В документе отражен еще один принципиальный момент. Нам удалось достичь правового компромисса по базовому подходу в отношении международно-правовых аспектов использования ИКТ. Этот компромисс заключен в сбалансированной формуле: международное право в целом применимо к информационному пространству, но при этом необходимо выработать и новые нормы, которые отражали бы его специфику.

Такой подход — не дипломатическая казуистика. Он продиктован соображениями здравого смысла. Первая часть этого компромисса фиксирует тот факт, что информационное пространство не является пространством хаоса, «джунглями», в которых не действуют общепринятые международные принципы и нормы. Едва ли кто-то станет отрицать, что государ-

ства при использовании ИКТ должны соблюдать положения Устава ООН. В докладе ГПЭ есть, например, четкое указание на то, что один из базовых принципов современного МП — принцип уважения государственного суверенитета — распространяется на сферу использования государствами ИКТ, в частности, юрисдикцию государств над ИКТ-инфраструктурой на их территории.

Однако у компромисса есть и вторая часть. Она предполагает выработку новых норм МП, которые учитывали бы специфические особенности ИКТ. Этому также есть логичное объяснение: информационное пространство, как новая сфера деятельности человека, не может «автоматически» регулироваться теми нормами, которые создавались для совершенно иных технологических условий. В прошлом по подобному пути шло развитие морского и космического права.

На данном этапе вырисовываются два основных направления развития международно-правовой базы — адаптация (в тех случаях, когда это возможно и целесообразно) ряда существующих норм и выработка новых. Необходимо закрыть международно-правовые «лакуны» в этой области.

Во-первых, это проблема релевантной терминологии. Такие базовые понятия МП как «вооруженное нападение», «акт агрессии», «нейтралитет» и др. применительно к информационному пространству могут получить совершенно иное правовое наполнение.

Например, может потребоваться расширенная интерпретация «акта агрессии», который определяется документами ООН как «применение вооруженной силы государством против суверенитета, территориальной неприкосновенности или политической независимости другого государства» (ст. 1, резолюция «Определение агрессии» Генассамблеи ООН 3314 от 14 декабря 1974 г.). В список действий, попадающих под определение «агрессии», включены вторжение вооруженных сил на территорию другой страны, оккупация, территориальная аннексия, бомбардировки, блокада морских портов и пр.

Очевидно, что данный список, составленный более тридцати лет назад в совершенно иных военно-политических и технологических реалиях, далеко не исчерпывающий. Резолюция предусматривает его расширение. Как представляется, в него можно было бы внести злонамеренное использование ИКТ, включая компьютерные атаки на критическую инфраструктуру. Конкретные формулировки в этом смысле, безусловно, требуют детальной проработки.

Примечательно, что под современное определение агрессии попадает в том числе:

a) «действие государства, позволяющего, чтобы его территория использовалась этим другим государством для совершения акта агрессии против третьего государства»;

b) использование наемников для применения вооруженной силы против другого государства.

Данные положения также могли бы быть адаптированы к информационному пространству. И у нас уже есть наработки в этой области. В упомянутом докладе ГПЭ прямо указано, что «государства не должны использовать посредников для совершения международно-противоправных деяний» с применением ИКТ, а также должны стремиться предотвращать использование их территории в незаконных целях.

Во-вторых, это проблема регулирования конфликтов в информационном пространстве с точки зрения jus ad bellum (право на применение силы) и jus in bello (международное гуманитарное право), в том числе квалификация информационного оружия как нового вида вооружений, реализация права на самооборону, включая параметры пропорционального ответа на нападение с использованием ИКТ и др.

Поясню на конкретном примере. В соответствии с Уставом ООН (ст. 51) применение силы возможно лишь в одном случае: при реализации права на самооборону. В свою очередь, это право получает государство, которое подверглось «вооруженному нападению». Конкретного определения «вооруженного нападения» МП не содержит. По сложившейся практике под ним понимается нападение с применением традиционных методов и средств ведения военных действий. В связи с этим возникает вопрос — можно ли классифицировать ИКТ как оружие? И если да, то к какому виду вооружений они могут быть отнесены? В случае «вооруженного нападения» государство имеет право на «пропорциональную» самооборону. Точных параметров «пропорционального ответа», даже в случае с традиционными методами ведения военных действий, установить не удалось до сих пор, хотя попытки предпринимаются на протяжении полувека. Очевидно, что определить «пропорциональность» самообороны применительно к сфере использования ИКТ будет еще сложнее.

С другой стороны, если ИКТ рассматривать как технологии двойного назначения, могут ли быть распространены на них ограничения в рамках соответствующих режимов?

Отдельного внимания заслуживает трактовка понятия «нейтралитет» применительно к информационному пространству. Например, может ли государство считаться нейтральным, если через его территорию ведутся компьютерные атаки на другое государство? Либо такие удары наносятся негосударственными субъектами в интересах третьей страны?

Кроме того, существует проблема международно-правовой ответственности за неправомерное применение государствами ИКТ, форм ее установления и закрепления. Как будут в случае с ИКТ урегулироваться возникающие споры, какую роль в этом должны играть механизмы ООН и в каком направлении их необходимо развивать — вот далеко неполный список возникающих в связи с этим вопросов.

Как было сказано выше, в июле проведет первое заседание новая ГПЭ ООН по МИБ. По российской инициативе ее мандат сфокусирован на двух темах — использование ИКТ в конфликтах и применимость МП к информационному пространству. Мы ожидаем от дискуссии в рамках данной ГПЭ конкретных выводов по данной проблематике.

В этом смысле встречи на экспертном уровне накануне новой сессии ГПЭ, подобные сегодняшней, могли бы сделать весомый практический вклад в ее работу. Возвращаясь к проблеме терминологии, хотелось бы обратить внимание на опыт ОБСЕ, где в настоящее время идет обсуждение предложенного Россией глоссария в сфере МИБ. Этот глоссарий подготовлен на основе всех действующих на данный момент соглашений по МИБ, участником которых является Россия.

Форум в Гармише заслужил высокий международный авторитет в плане дискуссии по вопросам МИБ и представляет целый ряд национальных взглядов на данную проблематику. Экспертный потенциал этой площадки мог бы иметь и конкретное применение в политической плоскости. Например, можно было бы создать в рамках Форума неформальную рабочую группу по выработке международно-правовой терминологической базы в сфере ИКТ. Такая группа могла бы систематизировать существующие понятия и определить направления их возможной адаптации. Итоги данной работы могли бы быть учтены в ходе дискуссии на профильных международных площадках, включая ООН.

N.V.Sokolova

Ministry of Foreign Affairs of the Russian Federation

On international legal aspects of the use of information and communication technologies: the experience of the UN Group of Governmental Experts on international information security

Ladies and gentlemen, colleagues!

I would like to thank the organizers of this meeting for the opportunity to discuss among experts such relevant and crucial problematics as international legal aspects of the use of information and communication technologies (ICT).

Frankly speaking, for politicians and diplomats this topic is largely a «terra incognita». ICTs, as nuclear technologies half a century earlier, opened a new era in the history of mankind. Now we must determine at international level the rules for «the game» in the information space — what with regard to nuclear sphere has not been done in time. As you know, it resulted in an arms race, limitation of which required tremendous efforts of international community.

The results of today's debate will determine whether «the game» in the information space will be honest.

The relevance of this conversation cannot be overemphasized. If before now the threats in the information sphere seemed though frightening, but a distant perspective, now it is obvious that the time of «preamble» has passed. It is time to move on to concrete solutions.

General recognition of this fact can be illustrated by the fact that International information security (IIS) has become a full-fledged, influential track in the UN, along with disarmament and other «classical» topics. Last year, the UN General Assembly resolution on the establishment of a new Group of Governmental Experts (GGE) on IIS was supported by an unprecedented number of countries (more than 40). Despite the budgetary challenges the UN is currently facing, not only did the funding in this area not suffer, but it had been increased: GGE will be holding four (instead of three, as it was before) extended meetings. The first of these will take place in July in New York.

Let me take advantage of our meeting in Garmisch, this unique opportunity to directly address the experts, and to describe the «areas

of concern» that we'll have to tackle in the GGE. Primarily, these are questions of international legal regulation of the information sphere.

As it turned out, it is easy to get lost on this road. As with our conversation, that until now has been focused entirely on the discussion of «The Tallinn Manual on the International Law Applicable to Cyber Warfare». You can get an impression that this is the only work in progress in this field, and it has no alternatives. The very definition of the problem leads to fundamental disagreement — the report is based on the thesis, that conflicts with the use of ICTs are inevitable, and it is impossible to prevent them. All subsequent analysis is built on the basis of these assumptions.

In this regard the question arises: then what is the point in generally expensive international debate, if we acknowledge in advance our own powerlessness and inability to prevent war in the information space?

On the other hand, isn't this experts' report drawing too much attention, when even the authors evaluate the findings as outdated?

Regarding the question of international law regulating the use of ICT we start far «from scratch» and not «from Tallinn». While some countries enthusiastically developed «rules of war» in the information space, Russia came forward with rules to prevent it.

In 2011, together with SCO partners, we circulated a draft «Guidelines in the sphere of IIS». At its heart lies the idea of prevention of conflicts with the use of ICTs, as opposed to their legalization. «Guidelines» in their spirit are the «gentlemen's agreement» between countries that are guided by common sense and not ideological guidelines and seek to ensure peace in the information space.

We still receive responses from other nation-states. It is encouraging that interest to this document on political forums increases over time.

Frankly, the «Guidelines» get critical acclaim as well, although no one managed to provide any specific justification why this document cannot become an international legal basis for regulating the behavior of states in the field of ICTs. It is often an impression that criticism is not so much related to the content, but to «allergy» to the initiative coming from SCO countries.

Therefore, the silence of the expert community is surprising, as it seems to be so keen on «Tallinn manual» that it — whether out of inertia, or intentionally — ignores alternative initiatives. Even more disappointing are estimates in the spirit of «I did not

read, but condemn nonetheless». Although real and scientifically substantiated comments of experts in particular could help refine the «Rules of Conduct» in a constructive way.

Now let's move to positive things.

We have been able to reach agreement on a lot of things at the highest international level. Last year in June, the previous UN GGE has finished its work. Sharp debates were held until the last moment. But they showed that in the face of the common threats consensus is possible even if there is a disagreement between parties on specific issues. As a result, the report was adopted, and definitively confirmed that all countries are interested in ICT development for peaceful purposes, and in prevention of conflicts caused by their use.

By general opinion of GGE experts, preventing confrontation caused by ICT use should be a «starting point» for our conversation in the future. This is especially important today, when questions of war and peace in the information space are actually put on the agenda.

The document reflects another important point. We managed to reach a legal compromise on basic approach to international legal aspects of ICT use. This compromise is reflected in a balanced formula: international law is generally applicable to the information space, but it is necessary to develop new rules that would reflect its specific features.

This approach is not a diplomatic casuistry. It is dictated by considerations of common sense. The first part of this compromise captures the fact that information space is not a space of chaos, «jungle», where no generally accepted international principles and norms exist. It is unlikely that anyone would deny that in the use of ICTs the nation-states must comply with the provisions of the UN Charter. For example, the report of GGE has a clear indication that one of the basic principles of modern international law — the principle of respect for state sovereignty — extends to the sphere of ICT use by nation-states, in particular to jurisdiction of nation-states over ICT infrastructure in their territory.

However, this compromise has another side. It implies the development of new norms of international law, which take into account the specific features of ICTs. And there is a logical explanation to this as well: information space, as a new sphere of human activity, cannot be «automatically» governed by the rules that were created for completely different technological conditions. In the past development of maritime and space law went along a similar path.

At this stage, there stand out two main directions of development of the international legal framework — adaptation (in cases where it is possible and appropriate) of a number of existing standards and development of the new ones. It is necessary to close international legal «deficiencies» in this area.

Firstly, it is the problem of relevant terminology. Such basic concepts of international law as «armed attack», «aggression», «neutrality» and others can get a completely different legal content with regard to information space.

For example, we may need an extended interpretation of the «act of aggression», which is defined in the UN documents as «the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State» (Article 1, of the «Definition of Aggression», UN General Assembly Resolution 3314 of 14 December, 1974). The list of actions that fall under the definition of «aggression» includes armed forces invasion of the other state's territory, occupation, territorial annexation, bombing, blockade of sea ports, etc.

Clearly, this list, compiled in completely different military-political and technological realities over thirty years ago, is not exhaustive. The resolution provides for its extension. It seems that the list could be extended by inclusion of misuse of ICTs, including cyberattacks on critical infrastructure. In this context specific language will, of course, require a detailed study.

It is noteworthy that current definition of aggression includes the following:

a) «the action of a State in allowing its territory... to be used by that other State for perpetrating an act of aggression against a third State»;

b) employment of mercenaries for the use of armed force against another State.

These provisions could also be adapted to the information space. And we already have experience in this field. The above-mentioned report of the GGE expressly states that «States must not use proxies to commit internationally wrongful acts» with the use of ICT and should seek to prevent the use of their territory for illegal purposes.

Secondly, there is a problem of conflict management in information space in terms of jus ad bellum (the right to use force) and jus in bello (international humanitarian law), including qualification of information warfare as a new type of weapon, and realization of the right to self-defense, including parameters of proportional response to the attack with the use of ICT, etc.

Let me provide a specific example. In accordance with the UN Charter (Article 51) the use of force is possible only in one case: the realization of the right to self-defense. This right is in turn given to the nation-state which suffered an «armed attack». International law does not provide a specific definition of an «armed attack». In accordance with established practice it is thought of as an attack by the use of traditional methods and means of warfare. In this regard, the question arises — is it possible to classify ICTs as a weapon? And if so, what weapon category should they be referred to? In case of an «armed attack», the state has the right to «proportional» self-defense. So far we couldn't establish exact parameters of «proportional response» even regarding traditional methods of warfare, although there have been attempts to do so over the course of the last fifty years. Obviously, it will be even harder to determine «proportionality» of self-defense in relation to the use of ICTs.

On the other hand, if ICTs are considered to be dual-use technologies, can these restrictions be extended to them under corresponding regulations?

Special attention must be given to interpretation of the concept of «neutrality» in relation to information space. For example, can nation-state be considered neutral if cyber attacks on another nation-state are conducted through its territory? Or if such strikes are launched by non-state actors in the interests of a third country?

There is also an issue of international legal responsibility for misuse of ICT by nation-states, and forms of allocation and consolidation of this responsibility. How will be settled the disputes involving the use of ICTs, what should be the role of the UN mechanisms and in what direction should they be developed — this is an incomplete list of new related questions.

As mentioned above, the first meeting of the new UN GGE will be held in July. At the initiative of Russia, its mandate focuses on two themes — the use of ICT in conflicts and the applicability of the International law to information space. We expect the discussions under this GGE to draw specific conclusions on these issues.

In this sense, such meetings of experts, as we have today, at the eve of the new session of the GGE, could make a significant practical contribution to its work. Back on issue of terminology, we would like to draw attention to experiences of the OSCE, where currently there are held discussions of the glossary on IIS proposed by Russia. This glossary has been developed on the basis of currently existing agreements on international information security, to which Russia is a party.

In terms of international information security discussions, the Forum in Garmisch has earned high international standing and represents a number of national views on these issues. Expertise of this platform could have particular application in the political arena. For example, an informal working group on elaboration of international-legal terminology in the sphere of ICT could be created as a part of the Forum. This group could systematize existing concepts and determine the directions of their possible adaptation. Results of this work could be taken into account during discussion within relevant international forums, including the United Nations.

Сюй Люнди

Китайский институт международных исследований

Факторы, оказывающие влияние на содержание понятия «Кибервойна»

I. Многообразие деятельности в Интернете и вопрос существования кибервойны

1. Многообразие деятельности в Интернете

Существует огромное разнообразие видов и направлений деятельности в Интернете. Также существует различное понимание людьми деятельности в киберпространстве, киберугроз и кибербезопасности. Например, некоторые люди считают, что можно выделить четыре вида Интернет-угроз: кибернападения, организованная преступность, идеологический и политический экстремизм, и кибервторжения, организованные государствами. Другие считают, что кибератаки это несанкционированные попытки доступа, атаки типа «распределенный отказ в обслуживании» (DDoS) и вредоносные программы. Как считают третьи, кибератаки включают в себя кибертерроризм, кибервойну, киберпреступность и кибершпионаж. При этом, хотя террористические организации и присутствуют в Интернете, истинный кибертерроризм попрежнему встречается крайне редко, также как пока не было и настоящей кибервойны. Напротив, наиболее актуальными проблемами являются киберпреступность и кибершпионаж. Одним словом, из-за сложного и постоянно меняющегося характера деятельности в Интернете и широкого спектра киберугроз необходимо сформулировать правила, чтобы противостоять этим угрозам и обеспечивать кибербезопасность.

Кибервойна является крайним проявлением онлайн-угроз и кибератак, и внимание к ней постоянно возрастает. Что интересно, с момента создания Интернета на международном уровне идёт постоянная дискуссия о кибервойне, а различные государства ведут борьбу за «доминирование» в сети. В ходе войны в Персидском заливе 1991 года, войны в Косово 1999 года и войны в Ираке 2003 года, киберинструменты показали свои истинные возможности. За последние годы мно-

гие государства предприняли различные меры: представили документы по политике в области киберпространства, сформулировали киберстратегии, создали киберкомандования и способствовали формированию кибервойск — всё делалось так, будто кибервойна может разразиться в любой момент.

Представляется, что некоторые кибератаки, произошедшие в последние годы, являются новыми доказательствами появления кибервойны. Нападение на Эстонию в 2007 году и вирус Stuxnet в 2010 году рассматриваются как новейшие случаи кибервойны. Первый из вышеприведённых примеров был охарактеризован министром обороны Эстонии как «прошедшая незамеченной Третья мировая война». Западные эксперты по вопросам кибервойны также называют его первой кибервойной в истинном смысле этого слова. Вирус Stuxnet не вывел из строя иранские ядерные объекты, но привёл к тому, что примерно двадцать процентов центрифуг Ирана было выведено из строя, что привело к огромным задержкам в реализации ядерной программы Ирана. Появление вируса Stuxnet означало возникновение еще одного типа кибероружия и начало нового этапа кибервойн.

2. Вопрос существования кибервойны

Люди по-разному определяют и понимают войну. И таким же образом по-разному понимается кибервойна. В целом, в настоящее время до сих пор нет единого мнения по вопросу существования кибервойны. Мнения в целом разделились на два лагеря: одна группа утверждает, что кибервойна существует и, более того, уже имела место быть; другая точка зрения заключается в том, что кибервойны не существует, и она не будет происходить.

Еще в 1993 году Джон Аркуилла и Дэвид Ронфелдт из Rand Corporation заявили «грядёт кибервойна!» В 2010 году заместитель министра обороны США Уильям Линн III, заявил «хотя киберпространство и является рукотворным», с точки зрения военных действий оно стало «таким же важным, как суша, море и воздух». Бывший «киберцарь» Белого дома Ричард Кларк считает, что угроза таких террористических актов, как атаки 11 сентября, меркнет в сравнении с угрозой, которую представляют кибервойны. Он призвал принять экстренные меры «для предотвращения катастрофы кибервойны». В феврале 2011 года бывший в то время директором ЦРУ Леон Панетта также предупредил «следующий Перл-Харбор

вполне может быть вызван кибератакой». Конечно, как считают некоторые, это своего рода «киберпаранойя» и избыточная реакция на кибератаки.

В противоположность «киберпаранойе», Томас Рид из Королевского колледжа Лондона считает, что, хотя многочисленные кибератаки и имели место быть, кибервойны до сих пор не было. Не было ни одного случая кибервойны в настоящее время, и невозможно, что она случится в будущем — поскольку агрессивное действие любого вида должно удовлетворять ряду условий, прежде чем оно будет представлять собой акт войны. Согласно определению Карла фон Клаузевица, война должна быть насильственной, инструментальной и преследовать политические цели или, иными словами, любой акт войны должен быть потенциально смертельным, инструментальным и политическим. Однако среди всех кибератак, которые уже были осуществлены, независимо от их масштаба, ни одна не удовлетворяет этим условиям и, таким образом, не является актом войны. Напротив, все прошлые и настоящие кибератаки, имеющие в своей основе политический интерес, могут быть отнесены к трем относительно сложным формам деятельности, которые являются такими же древними, как сама война: диверсии и шпионаж.

II. Факторы, оказывающие влияние на определение «кибервойны»

В условиях отсутствия консенсуса по концепции кибервойны, для точного определения и понимания вопроса, необходимо уточнить характеристики термина, в том числе определить нападающих и объекты атаки, задачи и последствия.

1. Злоумышленники и объекты атаки

Упрощённо, злоумышленники могут быть разделены на три категории: отдельные лица, группы и государства. Они могут взаимодействовать в шести парах: отдельные лица — отдельные лица, отдельные лица — группы, отдельные лица — государства, группы — группы, группы — государства и государства — государства. С точки зрения этих конфигураций, только атаки государств на государства могут быть охарактеризованы как акты войны, в то время как в других случаях было бы очень трудно охарактеризовать атаки таким образом. Конечно, если лицо или группа лиц уполномочены государством или действует по его приказу, это также мо-

жет представлять собой акт войны. Однако из-за уникальной природы самого киберпространства источник атаки сложно обнаружить. Таким образом, очень трудно идентифицировать злоумышленника и сделать вывод, что кибервойна действительно имеет место быть.

Что касается объектов атаки, это, как правило: компьютерные операционные системы и программно-аппаратные средства; программные ресурсы и информация, присутствующая на компьютерах, например, личная информация, корпоративные секреты и интеллектуальная собственность; и критически важные инфраструктуры, такие как банковские системы, коммуникации, системы авиакомпаний, плотин и электростанций. Эти объекты атаки могут принадлежать отдельным лицам, группам или государствам, находиться на разных уровнях и обладать разной ценностью. Поэтому используя только один фактор/критерий очень трудно определить, существует ли кибервойна. Этот Гордиев узел также существует в вопросе определения кибервойны с точки зрения атакующего или объекта атаки.

2. Цели и последствия кибератак

Так же как существуют различные виды деятельности в киберпространстве, существует огромное разнообразие целей, ради которых осуществляются кибератаки. Некоторые атаки осуществляются из чистого интереса и любопытства нападающего или для демонстрации компьютерного таланта и способностей — большинство первых опытов хакерской деятельности попадает под эту категорию. Целью некоторых атак является получение доступа к корпоративным секретам, экономическая выгода или онлайн-мошенничество. Некоторые из них осуществляются с целью саботажа, в том числе: порчи или удаления информации с компьютеров, порчи или нарушения работы программного обеспечения и операционной системы или выведения из строя аппаратного обеспечения или информационной инфраструктуры. Конечно, целью некоторых кибератак также является кибервойна, как в ограниченной, так и полномасштабной форме.

Соответственно, атаки, преследующие различные цели, приводят к различным последствиям, среди которых: потеря личной и коммерческой информации, хищение интеллектуальной собственности, саботаж компьютерного аппаратного и программного обеспечения, нарушение работы операци-

онной системы компьютера, уничтожение критически важной информационной инфраструктуры, и даже человеческие жертвы. Кроме человеческих жертв, все другие последствия имели место, но очень трудно воспринимать их как составляющие части кибервойны. Даже если атаки приводят к человеческим жертвам, их всё равно необходимо дифференцировать в зависимости от того, были ли они вызваны прямо или косвенно. Все эти факторы влияют на вопрос, состоялась ли кибервойна, и существует ли она как таковая.

Проще говоря, при анализе и оценке характера киберинцидентов, надо рассматривать вышеупомянутые факторы в совокупности. Необходим объективный анализ конкретной ситуации, в том числе виновника и жертвы нападения, целей, а также возможных последствий. Мы не должны преувеличивать или игнорировать факты. Также нужно избегать чрезмерного упрощения понимания кибервойны, когда все кибератаки сваливаются в одну кучу в категорию «военные действия».

Xu Longdi
China Institute of International Studies

Factors Influencing the Definition of 'Cyber Warfare'

I. The diverse nature of online activity and the contested existence of cyber warfare

1. The diverse nature of online activity

There is a huge amount of variety among the type and nature of online activities, and also differences among people's understanding of cyber activity, -threats and -security. For example, some people believe online threats can be divided into four levels: cyber intrusion, organized crime, ideological and political extremism, and cyber invasion originating from countries. Others believe cyber attacks include hacking, distributed denial of service (DDoS), and Trojan malware. Still others believe cyber attacks include cyber terrorism, cyber warfare, cybercrime, and cyber espionage. Among these, although terrorist organizations do have an online presence, true cyber terrorism is still extremely rare, while true cyber warfare is also yet to take place. In contrast, cybercrime and -espionage are the most pressing problems. In brief, because of the complex and ever-changing nature of online activity, and the wide range of cyber threats, it is imperative to formulate rules to tackle these threats and safeguard cyber security.

Cyber warfare is the extreme form of online threats and cyber attacks, and is receiving an increasing amount of attention. In fact, since the inception of the Internet, internationally, there has been constant debate about cyber warfare, with different countries contesting the 'dominance' over the net. In the 1991 Gulf War, 1999 Kosovo War and 2003 Iraq War, cyber tools came into their own. In recent years, many countries have taken various measures, unveiled rafts of cyber policy, formulated cyber strategy, set up cyber commands and strengthened the building of cyber forces as if cyber warfare were about to break out at any time.

Some of the cyber attacks that have taken place in recent years seem to have provided further evidence of the arrival of cyber warfare. The 2007 attack on Estonia and the 2010 Stuxnet virus are seen as the newest cases of cyber warfare. The former was de-

scribed by the Estonia's defence minister as the "unnoticed Third World War". Western cyber warfare specialists also called it the first cyber war in its true sense. The Stuxnet virus did not disable Iran's nuclear facilities, but it did cause approximately twenty per cent of Iran's centrifuges to be scrapped and caused huge delays to Iran's nuclear plans. The appearance of the Stuxnet virus signified the inception of yet another type of cyber weapon and a new phase of cyber warfare.

2. The contested existence of cyber warfare

People have different ways of defining and understanding warfare. Similarly, there are also different understandings of cyber warfare. On the whole, at present there is still no consensus as to the existence of cyber warfare, with opinion generally divided into two camps: one group maintains that cyber warfare exists and, indeed, has already occurred; the other school of thought contends that cyber warfare does not exist and will not occur.

As early as 1993, John Arquilla and David Ronfeldt of the Rand Corporation claimed 'Cyber warfare is coming!' In 2010, US Deputy Secretary of Defense, William Lynn III, wrote "although cyberspace is a man-made domain", in terms of military action, it has become "as important as land, sea and air". The White House's former cyber 'czar', Richard Clarke, believes the threat posed by cyber warfare dwarfs that posed by terrorist attacks such as 9/11 and has called for the adoption of a raft of measures "to begin to prevent the catastrophe of cyber warfare". In February 2011 then-Director of the CIA, Leon Panetta, also warned "the next Pearl Harbour may well be a cyber attack". Of course, some believe this is a kind of 'cyber paranoia' and an overreaction to cyber attacks.

In contrast to this 'cyber paranoia', Thomas Rid at King's College London believes that although there have been numerous cyber attacks, there has not yet been a cyber war. There has not been one at present and neither is it possible that one will occur in future. This is because one form of aggressive action must satisfy a number of conditions before it constitutes an act of war. According to Carl von Clausewitz's definition, war must be violent, instrumental and political or, that is to say, any act of war must be potentially fatal, instrumental and political. However, among cyber attacks that have already taken place, regardless of the scale, none have satisfied these conditions and thus cannot be said to constitute an act of war. In contrast, all past and present

political cyber attacks can be attributed to three relatively complex forms of activity, which are as old as warfare itself: subversion, espionage and sabotage.

II. Factors influencing the definition of 'cyber warfare'

Faced with a lack of consensus on the concept of cyber warfare, it is beneficial for an accurate definition and understanding of the issue by clarifying the parameters of the term, including attackers and targets, and objectives and consequences.

1. Attackers and targets

Put simply, attackers can be divided into three levels of actors: individuals, groups and states. These can be configured in six pairs as: individual-individual, individual-group, individual-state, group-group, group-state and state-state. In terms of these configurations, it is only the state-state attacks that can be described as acts of war, whereas it would be very hard to describe attacks among the other five pairs in this way. Of course, if an individual or group is authorised or instructed by a state, this could also constitute an act of war. However, because of the unique nature of cyberspace per se, it is difficult to trace the origins of an attack. Therefore, it is very hard to identify the attacker, and to infer whether cyber warfare does actually exist.

In terms of attackers' targets, these often include: computer operating systems and soft- and hardware; soft resources and computer information such as personal information, corporate secrets and intellectual property; and critical infrastructures such as banking system, airlines, communications, dams and power stations. These targets may be individual, group or state assets, of different levels and of different value. Therefore, it is very difficult to determine the existence of cyber warfare from just one factor/criterion. This is also a Gordian knot in defining cyber warfare from the perspective of attacker or target.

2. Objectives and consequences of cyber attacks

Just as with the different types of cyber activity, there is a huge variety of objectives of cyber attacks. Some attacks are purely borne out of the attackers' interest and curiosity, or to demonstrate their computer talents and abilities — the majority of early 'hacking' falls into this category. Some attacks are to gather corporate secrets, gain economic advantage or perpetrate online fraud. Some

are for sabotage, including: corrupting or deleting information from a target computer, corrupting or paralyzing the target computer's software and operating system or corrupting the computer's hardware or information infrastructure. Of course, some cyber attacks are also intended to launch cyber warfare, in both its limited and unlimited forms.

Related to this, attacks with different objectives will also bring about different consequences, including: loss of personal and commercial information, theft of intellectual property rights, sabotage of computer hard- and software, corruption of computer's operating system, destruction of key information infrastructure or even human casualties. Apart from the latter, i.e. human casualties, all of these other consequences have occurred, but it is very difficult to see them as constituting cyber warfare. Even if attacks result in casualties, these still have to be differentiated according to whether they were caused directly or indirectly. These factors all influence the decision as to whether cyber warfare has already taken place or whether it even exists.

Simply put, when analysing and evaluating the nature of cyber incidents, one must take an overview of the above-mentioned factors in a comprehensive manner. One must make an objective analysis of the specific situation, including the originator and victim of the attack, and the objectives, as well as possible consequences. We should not exaggerate or overlook facts, and should avoid oversimplifying cyber warfare by lumping all cyber attacks together under the rubric of 'acts of war'.

П.Л.Пилюгин

Институт проблем информационной безопасности МГУ имени М.В.Ломоносова

Проблемы создания технических средств контроля за соблюдением разрабатываемых норм международного права для киберпространства

Международный договор о запрете кибервойн

Существует разные определения для понятия «кибервойна». Часто это понятие связывают исключительно с сетью Интернет [1]: «компьютерное противостояние в пространстве Интернета» [2]. Более общее понимание распространяет это понятие на все компьютерные сети [5]. Нет и однозначного определения понятия «кибероружие».

Однако российские и американские специалисты в процессе работы над двусторонним проектом [4] пришли к общему пониманию целого ряда терминов [5]. В частности, было дано определение киберконфликта: «напряженная ситуация между и\или среди государств и/или политически организованных групп, при которой враждебные (нежелательные) кибератаки, провоцируют (приводят) к ответным действиям», а под кибервойной понимается: «высшая степень киберконфликта между или среди государств, во время которой государства предпринимают кибератаки против киберинфраструктур противника, как часть военной кампании». Еще более общее понимание киберугроз дается понятием «злонамеренного использования информационных и коммуникационных технологий (ИТК)» [6], которое включает в себя и киберпреступность, и кибертерроризм, а применительно к военным действиям позволяет рассматривать ИТК как «неявное оружие» [6].

Одновременно с развитием понятийного аппарата и осознанием возможных последствий кибератак рассматривался вопрос о регулировании отношений в киберпространстве, как в национальном, так и в международном масштабе. Научное сообщество выступило за необходимость такого регулирования [7], а ряд политологов высказывали противоположное мнение о международных договорах в «Дискуссионном клубе» U.S. News & World Report [8]. Однако в последнее время мнение о том, что «международный договор о запрете кибер-

войн — это единственный способ совладать с угрозой» [9], становится все более актуальным. Можно также согласиться с автором следующей цитаты, что хотя «полное запрещение кибервооружений — это, конечно, хорошая цель, но почти наверняка недостижимая. Более вероятны такие договоры, которые обяжут стороны воздерживаться от применения оружия первыми, запретят кибероружие «широкого спектра действия», а также обяжут иметь лишь такие вооружения, которые самоуничтожаются по окончании боевых действий. Договоры, ограничивающие тактику и задающие пределы для накопления вооружений, могли бы стать следующей фазой соглашений» [9]. Представляется, что в качестве первого реального шага в этом направлении должно быть не руководство [10] по ведению кибервойн, а адаптация современного международного права к сложившимся реалиям [6], которая может быть в дальнейшем развита в отдельную отрасль права. Вопрос только в том, существуют ли технические возможности — киберсредства, позволяющие адекватно понимать происходящее в киберпространстве для применения соответствующих правовых норм.

Задачи адаптации международного права Jus ad Bellum

Международное право предусматривает возникновение права на оборону, применение государством вооруженных сил для отражения агрессии или угрозы миру, при этом предполагается, что возникающий или ожидаемый ущерб должен быть не незначителен [6, 11]. Однако как распознать угрозу миру или агрессию в киберпространстве и оценить величину ущерба, как определить реальный источник угрозы? Можно выделить три основные проблемы.

Во-первых, хотя подобная задача оценки угроз и возможного ущерба рассматривается методами анализа рисков информационной безопасности, но эти результаты имеют больше методологическое, а не практическое значение. Несмотря на публикации о большом количестве компьютерных атак [12] и существование различных методик выявления угроз и оценки возможных потерь [13], все это, по мнению многих экспертов, в большой степени лишь «торговля страхом». «Методов оценки вероятности существует больше пяти. Методов оценки ущерба — больше трех десятков. Методик оценки рисков вообще под полсотни. А результат все равно никого не устраивает» [14]. Это связано с тем, что реальных киберинцидентов со сколь-нибудь значительным ущербом относительно немного, а

применительно к рассматриваемой тематике обычно вспоминают только Stuxnet [15] или DDOS-атаку на информационную систему эстонского правительства в 2007 г. На самом деле, вместо реальной оценки вероятности той или иной атаки мы можем располагать только экспертными оценками и это также справедливо в отношении ожидаемого ущерба.

Вторая проблема связана с выявлением истинной причины возникшего ущерба. Дело в том, что любое программное обеспечение (ПО) содержит ошибки, последствия которых могут быть катастрофическими. Именно поэтому в технологии создания программного обеспечения наряду с информационной безопасностью (security) рассматриваются задачи надежности, устойчивости и техники безопасности (safety). 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.

И наконец, в-третьих, необходимо выявить источник угрозы\агрессии. В упомянутых выше кибератаках виновность США и Израиля в создании кода Stuxnet так и не была доказана, а истинным виновником эстонской атаки оказалась не Россия [16]. Иногда возможно обнаружить источник сетевых DDOS-атак, которые в сети идут постоянно [17] и на сегодняшний день не считаются серьезной угрозой. 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.

Вместе с тем для адаптации существующих норм международного права необходима «атрибуция фактов противоправ-

ного применения силы и вооруженного нападения на основе злонамеренного использования ИКТ» [6] причем такая, что должны быть:

- «доверие к показаниям средств технической фиксации нарушений норм международных договоров со стороны участников спора;
- мониторинг всех событий, составляющих юридические факты, порождающие право индивидуальной или коллективной самообороны;
- объективность информации технических средств мониторинга и возможность их представления в качестве средства доказательства в Международном Суде при рассмотрении соответствующих споров» [6].

Как видно из описанных выше проблем, связанных с распознаванием угрозы (агрессии), определением ее причины и источника, обеспечить атрибуцию фактов противоправного применения силы и вооруженного нападения на основе злонамеренного использования ИКТ только техническими средствами не удастся. Необходимо будет проведение расследования по каждому такому инциденту и фиксация полученных доказательств. Именно в этом смысле можно «создать единую систему (возможно на базе соответствующих национальных и региональных систем) регистрации фактов угрозы силой или ее применения, а также «вооруженного нападения» посредством злонамеренного использования ИКТ» [6]. Однако, кроме мероприятий по организации таких расследований уполномоченными специалистами, необходимо предусмотреть единые 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 агрессии и их необходимо защищать в том числе и в рамках международного права.

Задачи адаптации международного права Jus in Bello

Право вооруженных конфликтов — исторически сложившаяся правовая система международного права, регулирующая поведение воюющих сторон в период вооруженных конфликтов. С точки зрения рассматриваемой проблемы адаптации норм права к применению в киберпространстве важно отметить, что «основная часть положений, закрепленных в источниках международного гуманитарного права, либо инвариантна к виду оружия, используемого в процессе военных действий, либо ориентирована на ограничение использования конкретных видов вооружения» [6]. Рассматривая первоочередные задачи адаптации международного гуманитарного права, приведенные в [6], можно выделить следующие задачи, требующие создания соответствующих технических решений, обеспечивающих:

- особый порядок цифровой идентификации информационных систем и телекоммуникационных сетей, защищаемых международным гуманитарным правом;
- ведение реестров и архивов, предусмотренных нормами международного гуманитарного права;
- запрет военного злонамеренного использования ИКТ против лиц и объектов, охраняемых нормами международного гуманитарного права, а также критически важных объектов глобальной, региональных и национальных инфраструктур, разрушение которых может привести к неоправданным человеческим жертвам, а также существенным негативным экологическим последствиям;
- сохранение нейтралитета государств, не участвующих в военных действиях;
- запрет некоторых видов злонамеренного использования ИКТ;
- особую систему сертификации программных и технических продуктов по требованиям противостояния злонамеренному использованию ИКТ.

Рассмотрим некоторые технические и организационные решения, которые можно предложить для решения этих задач.

Введение доменной зоны и создание реестров Web-ресурсов, защищаемых международным гуманитарным правом.

Очень часто говоря о кибератаках имеют в виду атаки на Интернет-сайты всемирной паутины — World Wide Web

(WWW). Сегодня многие специалисты считают защиту Web-ресурсов основным трендом информационной безопасности.

Для того, чтобы легко опознать Web-ресурсы реестров и архивов, лиц и объектов, охраняемых нормами международного гуманитарного права, можно ввести отдельную доменную зону. Отдельно можно рассматривать Web-ресурсы критически важных объектов глобальной, региональных и национальных инфраструктур, разрушение которых может привести к неоправданным человеческим жертвам, а также существенным негативным экологическим последствиям.

Способ 1

Для разных типов объектов можно ввести разные доменные зоны. Для создания этих доменных зон надо обратиться в ICANN и возложить на него (или орган под юрисдикцией ООН) функцию ведения реестра организаций, обратившихся за регистрацией в этих доменах. Такие специализированные доменные зоны сегодня существуют, например:

«Старые» домены верхнего уровня общего пользования:

- AERO — домен для авиационной отрасли;
- EDU — домен для образовательных учреждений США;
- MUSEUM — для музеев;

«Новые» — после открытия сводной регистрации доменов верхнего уровня:

MED — домен для медицины (люди и организации);
MEDICAL — то же;
HOSPITAL — для госпиталей
и другие.

Регистрация в этом реестре имени из этой доменной зоны должна проводиться только при предоставлении организациями документов, подтверждающих их статус организаций, защищаемых международным гуманитарным правом. При этом получение нового доменного имени в этой зоне не отменяет старого доменного имени, так как один сайт может иметь несколько доменных имен.

Способ 2

Для опознавания доменных имен организаций, защищаемых международным гуманитарным правом, можно ввести дополнительные записи в базы данных DNS.

Тип	Расшифровка	Код	Описание	Употребимость	RFC
A	Address	1	Соответствие между именем и IP-адресом	одна из самых часто используемых записей	RFC 1035
NS	Authoritative name server	2	Адрес сервера доменной зоны	DNS	RFC 1035
CNAME	Canonical name	5	Алиасы -одноуровневая переадресация	широко используется	RFC 1035
SOA	Start of authority	6	Указание на авторитетность	DNS	RFC 1035
PTR	Domain name pointer	12	Механизм переадресации	широко используется для IP-адресов	RFC 1035
MX	Mail Exchanger	15	Почтового шлюза для домена.	важна для SMTPкола,	RFC 1035
TXT	Text string	16	Запись произвольных данных	DNS-туннели	RFC 1035
AAAA	для IPv6	28	Адрес в формате IPv6	эквивалента A для IPV4	RFC 3596
LOC	Location information	29	Географическое местоположение	?	RFC 1876
SRV	Server selection	33	Указание на сервера для сервисов	Jabber, Active Directory	RFC 2782

В частности, запись TXT позволяет добавлять произвольные данные в описание домена, запись LOC может быть использована при определении нейтральных сторон, а запись SRV описывает наличие конкретного сервиса (например, сервиса опознавания, о чем подробнее будет сказано ниже). Внесение записей для опознавания в базы данных DNS может проводиться соответствующими регистраторами без участия ICANN, но только при предоставлении организациями документов, подтверждающих их статус организаций, защищаемых международным гуманитарным правом.

Способ 3

Внесение в корневой каталог каждого сайта файла со специальным именем (имя и структура файла могут быть описаны в соответствующем RFC), содержащим информацию о статусе организации, защищаемой международным гуманитарным правом. Хотя это способ наиболее простой, однако в этом случае затруднена проверка подтверждения статуса ор-

ганизаций, защищаемых международным гуманитарным правом. Было бы правильнее сочетать этот способ с описанными выше способами 1 или 2.

Создание реестров IP-адресов узлов сети Интернет, защищаемых международным гуманитарным правом

Определить по IP-адресу доменное имя (а следовательно, и «опознать» его) можно также по базе данных DNS (запись PTR), однако в общем случае IP могут не иметь соответствующих им доменных имен. Например, к сети Интернет могут быть подключены в качестве узлов сети международных гуманитарных организаций, сервера и сети медицинских учреждений, сети критически важных объектов глобальной, региональных и национальных инфраструктур, разрушение которых может привести к неоправданным человеческим жертвам, а также существенным негативным экологическим последствиям.

Все IP-адреса узлов таких организаций можно вносить в реестр организаций, защищаемых международным гуманитарным правом. Создание реестров можно возложить на регистраторов IP-адресов (или другой орган под юрисдикцией ООН). Регистрация в этом реестре IP-адресов должна проводиться только при предоставлении организациями документов, подтверждающих их статус организаций, защищаемых международным гуманитарным правом.

Информацию о принадлежности IP-адреса к реестру организаций, защищаемых международным гуманитарным правом, можно предоставлять через сервис whois (RFC 3912), используя доступ к публичным серверам баз данных (БД) регистраторов IP-адресов. К сожалению, информация о реальных владельцах IP-адресов может быть неточной, так как адреса выделяются, как правило, Интернет-провайдерам, информация о переданных ими в пользование IP-адресах может быть недоступна.

Введение стандарта опроса IP-адресов узлов сети Интернет, защищаемых международным гуманитарным правом

Для опознавания узлов сети Интернет, защищаемых международным гуманитарным правом, можно разработать протокол опроса на принадлежность к реестру IP-адресов организаций, защищаемых международным гуманитарным правом. В простейшем случае для реализации этого опроса можно

использовать протокол пользовательских датаграмм (UDP, RFC 768) и зарезервировать фиксированный номер порта. Используя UDP, компьютерные приложения могут посылать сообщение-запрос (датаграмму) другим узлам сети Интернет по IP-адресу с указанием зарезервированного номера порта, а защищаемый узел должен возвращать номер (возможно, подписанный электронной подписью-сертификатом соответствующего доверительного центра-регистратора) регистрации в реестре IP-адресов организаций, защищаемых международным гуманитарным правом, или игнорировать этот запрос.

Важно отметить, что предлагаемый подход может быть единственно работоспособным в случае нарушения целостности сети (отсутствии доступа к DNS, сервисам whois или другим реестрам) в результате возникшего конфликта.

Обеспечение сохранения нейтралитета государств, не участвующих в военных действиях

Для опознавания Web-ресурсов государств, не участвующих в военных действиях, достаточно использовать национальный домен страны, запись LOC в базе данных DNS или сервис whois (RFC 3912), использующий доступ к публичным серверам баз данных (БД) регистраторов IP-адресов и регистраторов доменных имен и предоставляющий информацию о владельце доменного имени или IP-адреса.

К сожалению, информация в этих БД может быть не полной или не соответствовать действительности, так как регистраторы доменных имен не осуществляют проверку информации, предоставляемой владельцами доменных имен, информация же об IP-адресах в этом случае может быть более достоверной (но не всегда полной), так как национальные (местные, региональные) провайдеры со своим пулом адресов, как правило, остаются на территории своего государства.

Следует иметь в виду, что приведенные выше примеры возможной технической реализации способов адаптации международного гуманитарного права применительно к киберпространству далеко не исчерпывают список возможных технических решений. Более того, они ориентированы прежде всего на существующий сегодня вариант сети Интернет, основанный на протоколы IPv4, а с широким внедрением более развитого протокола IPv6 появятся новые возможности технических реализаций рассмотренных выше задач.

Задачи организационно-правового обеспечения технических средств

Как уже отмечалось выше, для реализации предлагаемых способов опознавания, защиты от вероломства (фальсификации статуса организаций, защищаемых международным гуманитарным правом) и проведения расследования инцидентов необходимо соответствующее организационное и правовое обеспечение.

Единая система сертификации информационных систем и телекоммуникационных сетей, защищаемых международным гуманитарным правом

Для проведения расследования инцидентов необходимо ввести систему сертификации информационных систем и телекоммуникационных сетей, защищаемых международным гуманитарным правом, предусматривающую:

- наличие минимально необходимого набора средств информационной безопасности;
- ведение средств регистрации информации, достаточной для анализа инцидентов;
- использование официально приобретенного сертифицированного ПО.

Сертифицированное ПО должно удовлетворять следующим условиям:

- 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.

Организационное и техническое обеспечение проведения расследований инцидентов

Должен быть создан международный орган (под юрисдикцией ООН) для проведения проверок информации, предоставляемой в реестре, проведения расследования инцидентов злонамеренного использования ИТК и расследования случаев появления средств ИТК (программных\аппаратных), имеющих назначение злонамеренного использования (кибероружие).

Орган должен иметь высокий экспертный статус, опираться на соответствующее оснащение для проведения проверок

и расследований и хранения и предоставления доступа к их результатам.

Стандартизация технических требований

Для реализации большинства перечисленных выше технических решений необходимо дополнить или разработать новые документы RFC (*Request for Comments*) и обеспечить их введение в общее пользование. Например, уже сейчас можно значительно сократить опасность DOS и DDOS атак, обязав провайдеров фильтровать не только входящий трафик (защита ресурсов от DOS-атак), но и исходящий (обезвреживание источников DOS-атак) трафик в соответствии с RFC2267 и RFC-2827.

В заключение хотелось бы отметить, что приведенный выше и далеко неполный, список технических и организационных мер описывает предложения, которые обладают не только разной сложностью реализации и требуют разных по величине издержек, но и эффективность их может существенно меняться в зависимости от стадий, остроты и глобальности киберконфликтов.

Литература

1. Український центр політичного менеджменту — Зміст публікації — Конвенция о запрещении использования кибервойны. http://www.politik.org.ua/vid/publcontent.php3?y=7&p=57

2. Кибервойна. http://ru.wikipedia.org/

3. Clarke, Richard A. *Cyber War*, HarperCollins (2010)

4. Двусторонний проект: Основы критически важной терминологии. К.Ф.Раушер, В.Ященко. МГУ им. М.В.Ломоносова 2013. http://iisi.msu.ru/articles/article31/

5. The Russia − U.S. Bilateral on Cybersecurity − Critical Terminology Foundations, Issue 2

6. Стрельцов А.А. «Основные направления прогрессивного развития международного права вооруженных конфликтов» МГУ им. М.В.Ломоносова 2014. http://iisi.msu.ru/articles/

7. «В поисках кибермира». Международный союз электросвязи и Всемирная федерация ученых. Geneva 2011. (Перевод на русский В.Бритков, В.Цигичко и др.)

8. «Дискуссоный клуб» U.S. News & World Report. http://www.3dnews.ru/632012/

9. «An International Cyberwar Treaty Is the Only Way to Stem the Threat» by Bruce Scheider, Security Technologist and Author June, 2012 http://www.usnews.com/debate-club/should-there-be-an-international-

treaty-on-cyberwarfare/an-international-cyberwar-treaty-is-the-only-way-to-stem-the-threat

10. The Tallinn Manual on the International Law Applicable to Cyber Warfare. General editor Michael N. Schmitt. Cambbridge University Press 2013. http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=5903855/1802381

11. Cyber-Weapons, Thomas Rid, Peter McBurney. The RUSI Journal molume 157, Issue 1, pp 6-13, 2012.

12. *ЛК: 45% киберугроз в 2013 году исходило от России и США,* 16 декабря, 2013. http://www.securitylab.ru/news/448558.php

13. Анализ инструментальных средств оценки рисков утечки информации в компьютерной сети предприятия. С. Лопарев, А. Шелупанов. «*Вопросы защиты информации», № 4, 2003.*

14. *Как считать риски? А.В.Лукацкий.* http://lukatsky.blogspot.ru/2012/04/blog-post_18.html

15. *W32.Stuxnet Dossier. Nicolas Falliere, LoamO Murchu, Eric Chien. Symatiec Security Response. Version 1.4* (*February 2011*)*/*

16. *Шнайер: тинейджеры и переговоры — наше спасение от кибервойны* (*Intel Live 2011 Лондон*) 01.12.2011 http://www.xakep.ru/57907/

P.L.Pilyugin

Institute of Information Security Issues MSU

Challenges of creating the technical control means for observance of future international law norms for cyberspace

There are different definitions of «cyberwar» concept. This concept is often linked solely to the Internet [1]: «computer confrontation on the Internet» [2]. More general understanding of this concept extends it to all computer networks [5]. Also there is no unambiguous definition of «cyber weapons» concept.

However, Russian and American experts in the course of a bilateral project [4] arrived at a common understanding of a number of terms [5]. In particular, there has been developed a definition of cyber conflict as «a tense situation between or among nation-states or organized groups where unwelcome cyber attacks result in retaliation», and refers to cyber war as «an escalated state of cyber conflict between or among states in which cyber attacks are carried out by state actors against cyber infrastructure as part of a military campaign». Yet more general understanding of cyber threats is as «malicious use of information and communication technologies (ICTs)» [6], which includes both cybercrime and cyberterrorism, and in relation to military action ICTs can be considered as «implicit weapons» [6].

Along with development of conceptual apparatus and realization of possible consequences of cyberattacks, consideration was given to the issue of regulation of relations in cyberspace, both nationally and internationally. The scientific community stood out for the need for such regulation [7], while a number of political analysts in the «Discussion Club» of US News & World Report [8] have expressed the opposite views of international treaties. Lately, however, the notion that «an international treaty banning cyberwar is the only way to cope with this threat» [9], is becoming increasingly important. You can also agree with the author of the following quote, that while «the total prohibition of cyber weapons is certainly a good goal, it is almost certainly unattainable. More likely are agreements which: oblige the parties to refrain from first use of such weapons; ban cyber weapons with «broad-spectrum attack»; and to have only such weapons, that will self-destruct at the end

of hostilities. The next phase could include agreements restricting tactics and defining limits of weapon stockpiles» [9] It seems that the first real step in this direction should be not a manual [10] for cyberwarfare, but adaptation of modern international law to the realities [6], which can be further developed into a separate branch of law. The only question is whether there are technical possibilities — cyber means — which will allow adequate understanding of what is happening in cyberspace for the application of the relevant legal standards.

Focal areas of Jus ad Bellum adaptation

International law provides for the exercise of the right to defense, the use of the armed forces by nation-states to repel aggression or thwart threats to peace. At that it is assumed that the resulting or expected damage must not be negligible [6,11]. But how to recognize a threat to peace or aggression in cyberspace, and to estimate damage, how to determine the real source of a threat? There are three major problems.

Firstly, although a similar problem of potential damage and threat assessment is considered by methods of information security risks analysis, these results have more methodological rather than practical significance. Despite reports on a large number of computer attacks [12] and the existence of different methods of identifying hazards and evaluating potential losses [13], according to many experts, to a large extent all of this is a «fear commerce». «There are more than five methods for estimating the probability. There are more than three dozens methods of damage assessment. There are no less than fifty risk assessment methods. And the result still satisfies no one» [14] This is due to the fact that there has been a relatively small number of actual cyberincidents with any significant damage. And considering the subject matter one usually only remembers Stuxnet [15] or DDOS-attack on the information system of the Estonian government in 2007. In fact, we can only have expertise rather than a realistic assessment of the likelihood of a particular attack — and this is also true with regard to expected damage.

The second problem relates to identification of the true cause of the actual damage. The fact is that any software (SW) contains errors, the consequences of which could be catastrophic. That is why software development technology considers, along with information security, the problems of reliability, stability and safety. 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 flaws or mistakes in programing rather than cyberweapons or backdoors. In the analysis of incidents all this requires a careful study of software code and in absence of human-readable source code, the complexity of this problem is comparable to creation of similar software.

And finally, thirdly, it is necessary to identify the source of threat\aggression. In the above-mentioned cyberattacks, the alleged involvement of the United States and Israel in creation of Stuxnet code has not been proved, and in case of Estonia the real author of the attacks was not Russia. [16] Sometimes it is possible to detect the source of network DDOS-attacks, which are constantly conducted on the network [17] and as of now are not considered a serious threat. Typically, they are conducted by hacker groups and not cybertroops of nation-states. And targeted attacks are much more complicated. The fact is that all of the existing «intrusion detection» systems actually only detect 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.

However, the adaptation of existing international law necessitates such «attribution of the facts of the wrongful use of force or armed attack by malicious use of ICT» [6] that there is:

- «confidence of the parties in dispute in the credibility of the evidence provided by technical means of detection of international agreements violations;
- monitoring of all events that make up legal facts that invoke the right of individual or collective self-defense;
- objectivity of the information provided by technical means of monitoring and possibility of its submission as proof to the International Court in consideration of related disputes»[6].

As is evident from the abovementioned issues associated with the recognition of the threat (aggression), determination of its cause and source, it will be impossible to attribute the evidence of the wrongful use of force or armed attack by malicious use of ICT only by technical means. For each such incident it will be necessary to conduct an investigation and secure the obtained evidence. In this sense precisely it is possible to «create a unified system (perhaps on

the basis of the relevant national and regional systems) for registration of the facts of the threat or use of force, as well as an "armed attack" by means of malicious use of ICT». [6] However, besides the framework for such investigations by authorized personnel, it is necessary to provide uniform requirements for 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, in particular within international law.

Focal areas of Jus in Bello adaptation

The Law of armed conflict is a historically developed legal framework of international law governing the conduct of belligerents in times of armed conflict. From the standpoint of rules of law adaptation to cyberspace it is important to note that «the major portion of the provisions enshrined in the sources of international humanitarian law, is either invariant to the type of weapon used in the course of hostilities, or focused on the restriction of the use of specific types of weapons»[6]. Considering the priorities of international humanitarian law adaptation, provided in [6], we can identify the tasks that require the establishment of appropriate technical solutions that provide:

- a special procedure of digital identification of information systems and telecommunications networks, protected by international humanitarian law;
- maintenance of registers and records, prescribed by the rules of international humanitarian law;
- the prohibition of military malicious use of ICTs against persons and objects protected under international humanitarian law, as well as critical objects of global, regional and national infrastructures, the failure of which could lead to unnecessary loss of human life, as well as significant environmental backlash;
- protection of neutrality of the states not participating in the hostilities;

- the prohibition of certain types of malicious use of ICTs;
- a special software and hardware certification system in compliance with requirements of countering the malicious use of ICTs.

Let's review some of the technical and organizational solutions that can be offered to meet these challenges.

The introduction of domain extension and the creation of registries of Web-resources protected under international humanitarian law.

Speaking of cyberattacks, one very often implies attacks on websites of the World Wide Web (WWW). Today many experts consider the protection of Web-resources a basic trend of information security.

In order to easily identify the Web-resources of registers and archives, persons and objects protected under international humanitarian law, it is possible to introduce a separate domain extension. Web-resources of global, regional and national critical infrastructures, the failure of which may result in unnecessary loss of human life, as well as a significant negative environmental backlash, can be considered separately.

Method 1

For different types of objects one can introduce different domain extensions. To introduce these domain extensions one should contact ICANN and entrust it (or a body under the jurisdiction of the UN) the function of keeping the register of organizations that applied for registration in these domains. Such specialized domain extensions exist today, for example:

The "old" top-level general use domains:

- AERO — the domain for the aviation industry;
- EDU — the domain for educational institutions in the USA;
- MUSEUM — for museums;

"New" — after the opening of consolidated top-level domains registration:

- MED — domain for medicine (people and organizations);
- MEDICAL — the same;
- HOSPITAL — for hospitals;
- and others.

Registration in this domain extension should be carried out only upon the presentation of documents, confirming the status of organizations that are protected under international humanitarian law. In this case, getting a new domain name in this extension does not negate the old domain name, as one website can have multiple domain names.

Method 2

For the identification of domain names of organizations that are protected by international humanitarian law, you can enter additional records in DNS database.

Type	Long form	Code	Description	Usage	RFC
A	Address	1	Consistence between the name and the IP-address	one of the most commonly used entry	RFC 1035
NS	Authoritative name server	2	Address of the server domain zone	DNS	RFC 1035
CNAME	Canonical name	5	Aliases — single-level forwarding	widely used	RFC 1035
SOA	Start of authority	6	Credibility indication	DNS	RFC 1035
PTR	Domain name pointer	12	Forwarding framework	widely used for IP-addresses	RFC 1035
MX	Mail Exchanger	15	Mail gateway for the domain	important for SMTP	RFC 1035
TXT	Text string	16	Acceptance of random data	DNS-tunnels	RFC 1035
AAAA	for IPv6	28	IPv6 address format	'A' value for IPV4	RFC 3596
LOC	Location information	29	Geographical location	?	RFC 1876
SRV	Server selection	33	Servers reference for services	Jabber, Active Directory	RFC 2782

The TXT record in particular allows you to add arbitrary data to the description of the domain, LOC record can be used to identify neutral parties, and SRV record describes the existence of a specific service (e.g., identification service, of which more will be said below). Adding records to the DNS database for identification can be carried out by the relevant Registrar without participation of ICANN, but only upon presentation of the document, confirming the status of organizations protected by international humanitarian law.

Method 3

Adding to the root directory of each website a file with a special name (first name and file structure can be described in the relevant RFC) containing information on the status of the organization,

which is protected by international humanitarian law. Although this method is the easiest, in this case it will be difficult to confirm the status of organizations that are protected by international humanitarian law. It would be better to combine this method with the above described method 1 or method 2.

Creation of registers of Internet nodes (their IP-addresses), protected by international humanitarian law.

A domain name can be identified (and hence "recognized") by its IP-address and DNS database (PTR record), but in general IPs may not have the corresponding domain name. For example, networks of international humanitarian organizations, servers and network of medical institutions, networks of global, regional and national critical infrastructures, the destruction of which may lead to unnecessary loss of human life, as well as a significant negative environmental backlash, can be connected to the Internet as nodes.

All IP-addresses of nodes of such organizations can be added to the register of organizations that are protected by international humanitarian law. Creation of registers could be entrusted to registrars of IP-addresses (or other agency under the jurisdiction of the United Nations). Registration in this register of IP-addresses should only be done upon presentation of documents confirming the status of organizations that are protected by international humanitarian law.

It is possible to provide information whether IP-address belongs to the register of organizations that are protected by international humanitarian law, through Whois service (RFC 3912), using the public access to the database servers (DB) of IP-addresses registrars. Unfortunately, information about the real owners of IP-addresses may be inaccurate, since, as a rule, addresses are allocated to Internet service providers, and information about IP-addresses distributed by them may be unavailable.

Introduction of polling standard for IP-addresses of Internet nodes, protected by international humanitarian law.

For identification of websites on the Internet, protected by international humanitarian law, it is possible to develop a polling protocol to determine if they are included in the registry of IP-addresses of organizations that are protected by international humanitarian law. The simplest case of polling implementation can use User Datagram Protocol (UDP, RFC 768) and reserve a fixed port number. Using UDP, computer applications can send a service request message (datagram) specifying the reserved port number to other websites on the Internet at specific IP-address.

Protected node should then either return a registration number (possibly signed by electronic signature certificate of appropriate trusted registrar center) in the registry of IP-addresses of organizations that are protected by international humanitarian law, or ignore the request.

It is important to note that the proposed approach may be the only functional way in the event of network integrity violation (no access to DNS, whois service, or other registers) as a result of a conflict.

Protection of neutrality of the states not participating in the hostilities.

For identification of Web-resources of the States not participating in hostilities, it is sufficient to use the national domain of the country, LOC record in the DNS database or Whois service (RFC 3912), that has access to public database servers (DB) of IP-addresses registrars and domain names registrars, and provides information about the owner of a domain name or IP-address.

Unfortunately, the information stored in these databases may be incomplete or may not correspond to reality, since the domain name registrars do not carry out verification of the information provided by the owners of the domain name, and information about IP-addresses in this case may be more accurate (but not necessarily complete), because national (local, regional) ISPs and their address pool tend to remain in the territory of the state.

Objectives for organizational and legal support of technological tools

As noted above, the implementation of the proposed methods of identification, protection against treachery (falsification of status of organizations that are protected under international humanitarian law) and incidents investigation must have an appropriate organizational and legal support.

Unified system of certification of information systems and telecommunications networks that are protected by international humanitarian law

To investigate incidents we need to introduce a system of certification of information systems and telecommunications networks that are protected by international humanitarian law. This system should consider:

- availability of a baseline information security tools;
- maintaining means of information recording sufficient for incidents analysis;
- use of officially purchased certified software.

Certified software must meet the following specifications:

- 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 is stored.

Organizational and technical support for investigations of incidents

An international body (under the jurisdiction of the United Nations) should be created to perform audits of information provided in the registry, investigate incidents of malicious use of the ICTs and investigate occurrences of ITCs (software\hardware) intended for malicious use (cyberweapons).

This body should have a high expert status, use appropriate equipment to carry out inspections and investigations, storage and provide access to their findings.

Standardization of technical requirements

Most of the abovementioned technical solutions in their implementation necessitate supplement of existing or development of new RFC documents (Request for Comments) and their introduction into general use. For example, at the moment we can significantly reduce the risk of DoS and DDoS attacks if we make it obligatory for providers to filter not only incoming (protection of resources from DoS-attacks), but also outbound traffic (neutralizing sources of DOS-attacks) in compliance with RFC2267 and RFC-2827.

In conclusion, it should be noted that the abovementioned suggestions not only differ in complexity of their implementation and require different expenses, but their effectiveness may vary considerably depending on the stage, severity and scope of cyberconflict.

References

1. Український центр політичного менеджменту — Зміст публікації — Konventsia o zapreshenii kibervoini (Convention on prohibition of cyberwar). http://www.politik.org.ua/vid/publcontent.php3?y=7&p=57 (in Russian)

2. Kibervoina (Cyberwar). http://ru.wikipedia.org/ (in Russian)

3. Clarke, Richard A. *Cyber War*, HarperCollins (2010)

4. Двусторонний проект: Основы критически важной терминологии. К.Ф.Раушер, В.Ященко. МГУ им. М.В.Ломоносова 2013.

5. The Russia– U.S. Bilateral on Cybersecurity– Critical Terminology Foundations, Issue 2 http://iisi.msu.ru/articles/article31/

6. A.A.Streltsov «Osnovnie napravleniya progessivnogo razvitiya mezhdunarodnogo prava vooruzhennih konfliktov (Focal areas of progressive development of international law of armed conflict)» MSU, 2014. http://iisi.msu.ru/articles/

7. «V poiskah kibermira (In search of cyberworld)». ITU and World Federation of Scientists. Geneva 2011. (in Russian)

8. «Diskussionniy klub (Discussion club)» U.S. News & World Report. http://www.3dnews.ru/632012/ (in Russian)

9. «An International Cyberwar Treaty Is the Only Way to Stem the Threat» by Bruce Scheider, Security Technologist and Author June, 2012 http://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare/an-international-cyberwar-treaty-is-the-only-way-to-stem-the-threat

10. The Tallinn Manual on the International Law Applicable to Cyber Warfare. General editor Michael N. Schmitt. Cambbridge University Press 2013. http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=5903855/1802381

11. Cyber-Weapons, Thomas Rid, Peter McBurney. The RUSI Journal volume 157, Issue 1, pp 6-13, 2012.

12. *LK: 45% kiberugroz v 2013 godu ishodilo ot Rossii I SSHA* (*LK: 45% of cyberthreats in 2013 came from Russia and the USA*), *December* 16, 2013. http://www.securitylab.ru/news/448558.php

13. Analiz instrumentalnikh sredstv otsenki riskov utechki informatsii v kompiuternoy seti predpriatiya (Analysis of instrumential tools of risk assessment of information leak in enterprise network) S.Loparev A.Shelupanov «Voprosi zashiti informatsii (Issues of information protection)*», № 4, 2003.*

14. *Kak schitat' riski?* (*How to calculate risks?*) *A.V.Lukatskiy* http://lukatsky.blogspot.ru/2012/04/blog-post_18.html

15. *W32.Stuxnet Dossier. Nicolas Falliere, LoamO Murchu, Eric Chien. Symatiec Security Response. Version 1.4* (*February 2011*)*/*

16. *Schnaier: tineidgeri I peregovori — nasche spasenie ot kibervoini* (*Schnaier: teenagers and negotiations — our salvation from cyberwar*) (*Intel Live 2011 London*) 01.12.2011 http://www.xakep.ru/57907/

Лоран Жизель[1]

Международный Комитет Красного Креста

Как международное гуманитарное право налагает ограничения на ведение кибервойны и предоставляет защиту гражданским лицам?

Ученые, предприниматели и правительства постоянно стремятся изобрести и разработать новые технологии, которые смогут дать огромные преимущества человечеству в экономической и социальной сферах. Технологические разработки в области информатики и коммуникации — и особенно создание и расширение киберпространства, что является одним из определяющих направлений технологического развития в последние десятилетия — не являются исключением в этом отношении. Но новые технологии вызывают и новые опасности и могут быть причиной серьезной обеспокоенности в самых различных областях, в частности, если они используются во время вооруженных конфликтов.

Впервые государства наложили ограничения на выбор средств и методов ведения войны, заключив в 1868 г. международный договор — Санкт-Петербургскую декларацию, согласовав технические границы, «в которых потребности войны должны остановиться перед требованиями человеколюбия», и предусмотрев возможность заключать новые соглашения в случае «усовершенствований, произведенных науками в вооружении войск», для согласования «между собою требований войны и законов человеколюбия». В духе важных принципов, нашедших воплощение в Декларации, и в соответствии со своим собственным мандатом МККК осуществляет мониторинг развития новых технологий и их использования или потенциального использования во время вооруженных конфликтов, например, использования беспилотных летательных аппаратов, снаряженных БЧ, автономных систем оружия или как раз военных действий в киберпространстве. Цель МККК заключается в том, чтобы оценить их реальное и потенциальное воздействие на людей и проанализировать, каким образом нормы МГП регулируют их использование. Применение

[1] Мнения, высказанные в настоящей статье, принадлежат исключительно ее автору и не обязательно отражают точку зрения МККК.

уже существующих правовых норм в отношении новой технологии ставит и вопрос о том, являются ли нормы достаточно ясными и четкими в свете специфических характеристик конкретной технологии и ее ожидаемого воздействия на человека.

Коммерческие предприятия, средства массовой информации и правительства регулярно сообщают о том, что их вебсайты и компьютерные сети подверглись кибернападениям. Однако нет авторитетного определения понятия «кибернападение» или «кибервойна», и разные люди, употребляя эти термины, имеют в виду разные вещи. Большая часть операций, которые обозначаются словами «кибернападение», является незаконным сбором информации — например, промышленным шпионажем — или другими киберпреступлениями и имеет место вне контекста вооруженных конфликтов. Такие случаи не регулируются международным гуманитарным правом (МГП). Выражение «кибервойна» используется в настоящей статье для обозначения средств и методов ведения военных действий, которые являются операциями, направленными против компьютера или через компьютер или компьютерную сеть путем информационного потока, когда такие операции в киберпространстве осуществляются в контексте вооруженного конфликта по смыслу МГП[2]. СМИ и обозреватели также часто говорят об «информационной войне». Информационная война была определена в Соглашении между правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности[3], а США дают определение информационных операций[4].

---

[2] См. ICRC 'How is the Term "Armed Conflict" Defined in International Humanitarian Law?', Opinion paper, March 2008, available at http://www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf

[3] Приложение 1. Перечень основных понятий в области обеспечения международной информационной безопасности: "Информационная война — *противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны*". Доступно по адресу: http://www.mid.ru/BDOMP/spm_md.nsf/0/CA43ABC67EDADF8644257BE8001D9047 (все ссылки на веб-сайты проверены 16 июня 2014 г.).

[4] Словарь военных и связанных с ними терминов Министерства обороны США('Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02') (с поправками от 15марта 2014 г.): "информационные опе-

Хотя даются разные определения, которые могут отражать серьезные различия в понимании этих понятий, представляется, что информационная война и информационные операции являются более широкими понятиями, чем кибервойна, как она определена здесь, и часто включают, по крайней мере, ее часть.

Особую озабоченность вызывает у МККК кибервойна из-за уязвимости киберсетей и потенциальной опасности, которую кибернападения представляют для людей. Если совершено нападение на сети государства, гражданские лица могут остаться без питьевой воды, медицинского обслуживания и электроэнергии, которые совершенно необходимы для нормальной жизни. Если система GPS парализована, могут иметь место жертвы среди гражданского населения — например, из-за нарушений в управлении полетами спасательных вертолетов. Хотя военный потенциал киберпространства еще понят не до конца, эксперты, как представляется, согласны с тем, что нападения на транспортные системы и сети электропередачи или даже на дамбы и ядерные установки вполне возможны с технической точки зрения. Такие нападения могут иметь очень далеко идущие последствия для благополучия, здоровья и жизни сотен тысяч людей.

Роль МККК заключается в том, чтобы напомнить, что во время вооруженного конфликта следует постоянно проявлять заботу с тем, чтобы щадить гражданских лиц и гражданские объекты. Действительно, кибервойна регулируется МГП, как и разработка любых новых видов оружия, средств и методы ведения войны. В киберпространстве нет правового вакуума. Это недвусмысленно установлено в Докладе Группы прави-

---

рации — *Комплексное использование во время военных операций информационных возможностей во взаимодействии с другими направлениями операции с целью воздействовать на процесс принятия решения противником или потенциальным противником, прервать или нарушить его или установить контроль над ним, обеспечивая защиту своему собственному*». http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (с. 127). Версия 2006 г. МО ('Joint Publication 3-13, Information Operations') (замененная версией 2012 г.) предлагает более подробное определение: "*информационные операции*»: *Комплексное использование основных возможностей электронной войны, операций компьютерных сетей, психологических операций, введения противника в заблуждение, мер обеспечения скрытности действий совместно с определенными поддерживающими и связанными с этим возможностям с целью воздействовать на процесс принятия решений противником — как со стороны человека, так и автоматизированным путем, прервать или нарушить его или установить контроль над ним, обеспечивая защиту своему собственному*». http://www.globalsecurity.org/intell/library/policy/dod/joint/jp3_13_2006.pdf (с. GL–9).

тельственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2013 г., в котором утверждается, что «международное право, и в частности Устав Организации Объединенных Наций, применимо и имеет важное значение для поддержания мира и стабильности и создания открытой, безопасной, мирной и доступной информационной среды»[5]. В документе Министерства обороны России 2011 г. «Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве» более конкретно заявляется, что Вооруженные Силы Российской Федерации обязаны соблюдать нормы МГП во время своих операций в информационном пространстве[6]. Все большее число государств, таких как Австралия, Канада, Япония, Нидерланды, Соединенное Королевство и США, а также международные организации, такие как Европейский Союз, также признают, что МГП применимо к кибервойне[7].

Основным принципом ведения военных действий является требование осуществлять нападения только на комбатантов и военные объекты. Любые нападения на гражданских лиц и гражданские объекты запрещены, и этот запрет распространяется на кибернападения. Во время вооруженного конфликта такие нападения будут в большинстве случаев являться нарушениями МГП. Действительно, системы водоснабжения питьевой водой и линии электропередачи, которые обслуживают гражданское население, банки, сеть железных дорог и инфраструктура здравоохранения являются в первую очередь гражданскими объектами (по крайней мере, до тех пор, пока они не становятся так называемыми объектами «двойного

---

[5] Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Записка Генерального Секретаря, 24 июня 2013 г., A/68/98, с. 8, ч. 19.

[6] Доступно по адресу: http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle.

[7] Австралия: A/66/152, с. 8, последний абзац; см. также: http://foreignminister.gov.au/speeches/2013/jb_sp_131017.html. Канада: A/68/156/Add.1, с 4, п. 2. Япония: A/68/156/Add.1,с. 18, первый абзац. Нидерланды: http://cms.webbeat.net/ContentSuite/upload/cav/doc/advies_22_reg_reactie_EN.pdf, с. 5. Соединенное Королевство Великобритании и Северной Ирландии: A/59/116, ч. 3 и A/65/154, ч. 7. США: A/59/116/Add.1 С.4, ч 5 и A/66/152 с 21-22; см. также на английском языке http://www.state.gov/s/l/releases/remarks/197924.htm. The European Union: E.U. Council Conclusions, General Affairs Council meeting, 25 June 2013, 12109/13, p. 4 para. 6 (available at http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2012109%202013%20INIT).

использования»). Как таковым, им предоставляется защита от непосредственных нападений. Системы водоснабжения, в частности, пользуются особой защитой, поскольку являются объектами, необходимыми для выживания населения[8]. Аналогичным образом, дамбы и гражданские атомные станции обычно не подпадают под определение того, что является военным объектом[9], и, таким образом, находятся под защитой от непосредственных нападений. Даже если они становятся военными объектами в конкретных обстоятельствах, МГП может тем не менее запретить нападения на них[10] или, по крайней мер, потребовать от стороны в конфликте, которая совершает такое нападение, проявить особую осторожность с тем, чтобы избежать высвобождения опасных сил и последующих серьезных потерь среди гражданского населения[11].

Однако подтверждение применимости МГП к кибервойне и напоминание о таких основополагающих нормах является лишь первым шагом. Ведь кибервойна поднимает целый ряд проблем для толкования и применения МГП[12].

Во-первых: анонимность. В киберпространстве очень легко обеспечить анонимность, что осложняет для государств дело присвоения агрессивной деятельности тем, кто ее осуществляет, особенно трудно это сделать своевременно. Поскольку МГП опирается на присвоение ответственности государствам и другим сторонам в вооруженном конфликте, анонимность

---

[8] Статья 54 Дополнительного протокола к Женевским конвенциям от 12 августа 1949 г., касающегося защиты жертв международных вооруженных конфликтов (Протокол I) от 8 июня 1977 г. (далее — ДП I) и МККК, Обычное международное гуманитарное право, т. I: Нормы. Жан-Мари Хенкертс и Луиза Досвальд-Бек. Обычное международное гуманитарное право, МККК, Москва, 2006. (далее — МККК. Исследование обычного права.), Норма 54 (на английском языке доступно по адресу: http://www.icrc.org/customary-ihl/eng/docs/v1_rul).

[9] Статья 52 ДП I и норма 8, МККК. Исследование обычного права. «Что касается объектов, то военные объекты ограничиваются теми объектами, которые в силу своего характера, расположения, назначения или использования вносят эффективный вклад в военные действия и полное или частичное разрушение, захват или нейтрализация которых при существующих в данный момент обстоятельствах дает явное военное преимущество».

[10] В силу принципа соразмерности или статьи 56 (1 и 2) ДП I.

[11] Статья 56(3) ДП I и норма 42, МККК. Исследование обычного права.

[12] Детальный анализ таких проблем можно найти в статье Cordula Droege, *Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians* in The International Review of the Red Cross, Volume 94, nb 886, summer 2012, pp. 533 — 578 (доступно по адресу: http://www.icrc.org/eng/assets/files/review/2012/irrc-886-droege.pdf)

создает большие проблемы. Если сторона, осуществляющая конкретную операцию в киберпространстве, не может быть идентифицирована, крайне трудно определить, применимо ли вообще МГП к этой операции. Ответ на этот вопрос может однако лежать не только в юридической плоскости, но в первую очередь в технической сфере.

Во-вторых: составляют ли операции в киберпространстве применение вооруженной силы, что обусловливает применимость МГП? Нет никакого сомнения в том, что вооруженный конфликт существует, когда операции в киберпространстве применяются наряду с традиционными кинетическими вооружениями. Однако когда первый — а, возможно, и единственный — враждебный акт является операцией в киберпространстве, может ли это приравниваться к вооруженному конфликту? Этот вопрос тесно связан — хотя и является отдельным — с вопросом о том, может ли только операция в киберпространстве считаться применением силы или вооруженным нападением в соответствии с Уставом Организации Объединенных Наций. Такие проблемы *jus ad bellum* очень важны и поэтому широко обсуждаются. Однако проблемы, связанные с *jus ad bellum* и вопрос о сфере применимости МГП (*jus in bello*) не следует смешивать. МГП применяется в ситуациях вооруженного конфликта как международного, так и немеждународного характера, как это определено в Женевских конвенциях 1949 г. и Дополнительных протоколах к ним 1977 г.[13] В этом отношении, как представляется, нет причин рассматривать кибероперации, воздействие которых будет аналогичным воздействию кинетических операций, иначе, чем последние. Такое разрушение важнейшей инфраструктуры, которое имеет долговременные последствия, что создает серьезные трудности для населения, может также считаться применением вооруженной силы, обусловливающим применимость МГП в свете его цели, заключающейся в предоставлении защиты гражданскому населению от таких последствий. Однако МККК считает, что только будущая практика государств сделает возможным определение того типа операций в киберпространстве, которые обусловливают применимость МГП при отсутствии каких-либо кинетических операций[14].

---

[13] См. ICRC ‘How is the Term “Armed Conflict” Defined in International Humanitarian Law?’, примечание 1 выше.

[14] ICRC, ‘International Humanitarian Law and the challenges of contemporary armed conflicts’, 31st International Conference of the Red Cross and Red Crescent, Geneva, 28 November–1 December 2011, Report prepared by the ICRC, October

В-третьих: в ситуациях, когда МГП применяется, например, если вооруженный конфликт уже ведется путем применения традиционных кинетических средств, встает вопрос об определение кибернападения. Понятие нападения является крайне важным для норм, касающихся ведения военных действий, особенно для принципов проведения различия, соразмерности и мер предосторожности при нападениях. Действительно, в то время как стороны в конфликте должны постоянно проявлять заботу о том, чтобы щадить гражданское население во время всех военных операций и предоставлять ему защиту от последствий военных действий, большинство конкретных обязательств, регулирующих ведение военных действий, касается «нападений». Дополнительный протокол I 1977 г. определяет нападения как «акты насилия в отношении противника, независимо от того, совершаются ли они при наступлении или при обороне» (Статья 49 (1)). Группа экспертов, которые составляли *Таллинское руководство по международному праву, применимому к кибервойне*, определили «кибернападение» в соответствии с МГП как «кибероперацию, независимо от того, совершается ли она при наступлении или при обороне, которая, как можно предположить на разумных основаниях, станет причиной ранений или смерти лиц или повреждения и уничтожения объектов»[15]. Суть дела, однако, заключается в деталях, а именно: что такое «повреж-

2011, 31IC/11/5.1.2, p. 37, para. 4, доступно по адресу: http://www.icrc.org/eng/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf.

[15] Tallinn Manual, Rule 30, p. 106, доступно по адресу: http://ccdcoe.org/tallinn-manual.html. Таллинское руководство было составлено по предложению Совместного центра кибернетической обороны НАТО. Однако Таллинское руководство не является доктриной НАТО, а лишь не налагающим обязательств документом, подготовленным группой экспертов в их личном качестве. Некоторые авторы высказываются негативно о Таллинском руководстве, потому что оно явилось попыткой, предпринятой на региональном уровне, и потому что оно может узаконить кибернетическую войну и способствовать милитаризации кибернетического пространства. Это, конечно, не является причиной того, что МККК принял участие в качестве наблюдателя в работе группы экспертов, которые его составляли. Цель участия МККК заключалась в том, чтобы проследить за тем, что в Руководстве обеспечивается защита, которую МГП предоставляет жертвам вооруженных конфликтов. МККК в целом согласен с формулировкой норм *jus in bello,* содержащейся в части Руководства, посвященной «праву кибернетических вооруженных конфликтов». Однако существуют исключения, когда МККК считает, что нормы действующего МГП сильнее или предоставляют больше защиты, чем нормы, которые содержатся в Руководстве. Более подробно см.: ICRC, 'What limits does the law of war impose on cyber attacks? Questions and Answers', 28

дение» в кибермире. Целый ряд экспертов в области МГП согласны с тем, что утрата функциональности объекта может также являться повреждением, хотя другие утверждают, что только физическое повреждение имеет отношение к делу. МККК придерживается того мнения, что если объект выведен из строя, не имеет значения, произошло это в результате уничтожения или каким-либо иным способом[16]. Этот вопрос очень важен на практике, поскольку более ограничительное определение нападения может означать, что меньшее число и менее четкие нормы МГП будут регулировать и, следовательно, налагать ограничения на операции такого типа. В частности, на операции в киберпространстве, цель которых заключается в том, чтобы вывести из строя гражданские системы, мог бы не распространяться запрет МГП, касающийся нападений на гражданских лиц и гражданские объекты, если «нападение» будет пониматься излишне ограничительно.

В четвертых: проблемы, которые создает явление взаимосвязанности киберпространства для норм МГП, предоставляющих защиту гражданскому населению и гражданским объектам. Существует только одно киберпространство, и те же самые сети, маршруты и кабели используются как гражданскими, так и военными пользователями. Как было отмечено Великобританией в прошлом году «Взаимосвязанный характер киберпространства означает, что совершение деструктивной деятельности в отношении одной системы может привести к непреднамеренным и непредсказуемым последствиям в других системах»[17]. Взаимосвязанность киберпространства может даже сделать невозможным проведение различия между военными и гражданскими компьютерными сетями при осуществлении кибернападения; если оно все-таки имеет место, такое нападение будет нарушать запрет на неизбирательные нападения. Использование вредоносных программных средств, которые бесконтрольно воспроизводятся и повреждают гражданские киберсети, также запрещено. Например, сторона в конфликте нарушит запрет на неизбирательные на-

---

June 2013, доступно по адресу: http://www.icrc.org/eng/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm.

[16] ICRC, 'Report on International Humanitarian Law and the challenges of contemporary armed conflicts', примечание 13 выше, с. 37, последний абзац.

[17] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. Доклад Генерального секретаря ООН, A/68/156, с. 20, первый абзац (ответ Соединенного Королевства Великобритании и Северной Ирландии).

падения в соответствии с МГП, если она запустит через Интернет вредоносное программное средство, предназначенное для того, чтобы заблокировать военные радары противника, предполагая при этом, что код этого вредоносного средства распространится и повлияет на работу радиолокационных станций управления гражданским воздушным движением. Согласно принципу соразмерности, сторона в конфликте должна сделать все практически возможное для того, чтобы понять, может ли нападение причинить случайный ущерб, который будет чрезмерным по сравнению с непосредственным и конкретным военным преимуществом, которое ожидается получить, и если это так, не осуществлять нападения. Более того, при нападении стороны в конфликте должны принять все практически возможные меры предосторожности с тем, чтобы избежать или, по крайней мере, свести к минимуму случайные потери среди гражданского населения и ущерб гражданским объектам, включая гражданские киберинфраструктуру и сети. Взаимосвязанность киберпространства влечет за собой опасность того, что кибернападения причинят случайный ущерб косвенным образом. Такой косвенный побочный ущерб, как бы он ни был отдален, должен быть принят во внимание в той степени, в какой его можно ожидать — и стороны в конфликте, которые планируют или осуществляют кибернападения, должны предусматривать опасность того, что может быть причинен косвенный побочный ущерб. Вопрос, кроме того, состоит в том, всегда ли возможно должным образом оценить такие косвенные последствия.

Это всего лишь краткий обзор проблемы, существует и множество других вызовов. Некоторые из них отражают проблемы, которые имеются в отношении кинетических операций, такие как определение понятия непосредственного участия в военных действиях. Если кто-то принимает непосредственное участие в военных действиях путем кибернападения в поддержку одной стороны в вооруженном конфликте, он не может ожидать бездействия от противника. Это лицо лишается своей правовой защиты от прямых нападений, включая кинетические нападения, во время осуществления кибернападения и подготовительных мер, которые являются его неотъемлемой частью. Другие вызовы, возможно, являются более специфическими для кибервойны, например, география киберконфликтов, применение права нейтралитета и понятия суверенитета или определение и правовой анализ кибероружия — это всего лишь некоторые из них.

Несмотря на эти трудные для решения проблемы, основной вопрос заключается не в том, являются ли новые технологии по своей сути хорошими или плохими. Новые технологии могут иметь и позитивное воздействие, если их применять, соблюдая нормы права. Что касается возможности избежать случайного ущерба гражданскому населению или гражданским объектам или свести их к минимуму, то боеприпасы с точным наведением, конечно, являются усовершенствованием по сравнению с артиллерией или воздушными бомбардировками, которые использовались во время Второй мировой войны. Нельзя недооценить существующие проблемы и вызовы, но нельзя исключать и возможности того, что технологическая эволюция может привести в будущем к разработке кибероружия, в результате применения которого при определенных обстоятельствах будет меньше потерь и меньше случайного ущерба, чем при использовании традиционного оружия, для достижения того же военного преимущества. Например, вполне вероятно, что кибероперация причинит меньше ущерба, чем бомбардировка, если цель и первой, и второй заключается в нарушении функционирования некоторых сетей коммунальных служб, которые используются как для военных, так и гражданских целей. В таких случаях принцип принятия мер предосторожности налагает обязанность на стороны в вооруженном конфликте выбирать, если это возможно, наименее опасные для гражданских лиц средства для достижения своей военной цели. При этом требуется целостный подход для того, чтобы внимательно рассмотреть со всех точек зрения все риски и возможные последствия применения новых технологий, и МККК призывает государства сделать это до принятия решения о разработке таких технологий. Хотя значимость МГП как основного корпуса права, которое налагает ограничения на кибервойну и предоставляет защиту гражданскому населению, должна быть подтверждена, МККК не исключает и возможности того, что потребуется развить право далее, чтобы гарантировать, что защита, которую оно предоставляет гражданскому населению, является достаточной. Это должны определить государства.

В связи с этим в международном сообществе ведется дискуссия относительно того, каким образом решать проблемы, поставленные кибервойной и, более широко, проблемы, связанные с информационной безопасностью. В 2011 г. Китай, Россия, Таджикистан и Узбекистан представили Генеральному секретарю Организации Объединенных Наций проект

Правил поведения в области обеспечения международной информационной безопасности[18], к числу авторов которого впоследствии присоединились Казахстан и Кыргызстан[19]. Кроме того, Россия предложила Проект Конвенции по международной информационной безопасности (Концепция)[20], и для России одной из приоритетных задач в области международной информационной безопасности является содействие формулированию и принятию государствами — членами Организации Объединенных Наций международных правовых актов, регламентирующих применение принципов и норм международного гуманитарного права при использовании информационных и коммуникационных технологий[21]. Со своей стороны Соединенное Королевство считает, что многосторонний инструмент, ограничивающий использование информационных технологий во время вооруженных конфликтов, не является необходимым именно потому, что право вооруженных конфликтов уже регулирует такое использование[22]. Несколько других государств высказали свое мнение по некоторым из проблем, поставленных применением и толкованием международного права в отношении кибервойны[23]. В декабре 2013 г., давая поручение Генеральному секретарю создать новую Группу правительственных экспертов, Генеральная Ассамблея добавила к тем вопросам, которые предстояло рассмотреть, вопросы «использования информационно-коммуникационных технологий в конфликтах и того, как международное право применяется к использованию информационно-коммуникационных технологий государствами"[24]. Хотя некоторые из этих документов и заявлений шире по своему охвату, чем МГП, МККК приветствует интерес, проявленный к этим вопросам.

---

[18] Доступно по адресу: http://nz.chineseembassy.org/eng/zgyw/t858978.htm.

[19] См. A/68/98, с. 10, ч. 18.

[20] Доступно по адресу: http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument.

[21] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. Доступно по адресу: http://www.scrf.gov.ru/documents/6/114.html (ч. 12(г.)).

[22] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. Доклад Генерального секретаря ООН, A/59/116, с. 13, ч. 3 (ответ Соединенного Королевства Великобритании и Северной Ирландии)

[23] См. ссылки в примечании 6 выше.

[24] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. A/RES/68/243, 27 декабря 2013 г., п. 4.

Международный Комитет готов и впредь предоставлять свои экспертные знания по вопросу о том, каким образом МГП налагает ограничения на кибервойну, с тем чтобы снизить уровень потенциальной опасности для людей и наилучшим образом заниматься поисками решения проблем, которые она поставила.

Однако эти проблемы подчеркивают необходимость того, чтобы стороны в вооруженных конфликтах проявляли повышенную осторожность, если и в то время когда они прибегают к кибернападениям, для того чтобы избежать ущерба, причиняемого гражданским лицами и гражданским сетям. Эти проблемы подчеркивают и важность того, чтобы государства, способные создать или приобрести средства для ведения кибервойны — как для наступательных, так и оборонительных целей, — провели оценку их законности в соответствии с МГП, как это необходимо сделать в случае любых других видов оружия или средств и методов ведения войны. Это требуется согласно статье 36 Дополнительного протокола I 1977 г.[25], и является единственным способом гарантировать, что вооруженные силы и другие государственные учреждения, которые могут во время вооруженного конфликта прибегнуть к методам кибервойны, сумеют соблюдать свои обязательства в соответствии с международным правом. Тот факт, что все возрастающее число государств работают над созданием возможностей для ведения кибервойны, только подчеркивает настоятельную необходимость найти решения этих задач.

---

[25] Статья 36 ДП I — Новые виды оружия: *При изучении, разработке, приобретении или принятии на вооружение новых видов оружия, средств или методов ведения войны Высокая Договаривающаяся Сторона должна определить, подпадает ли их применение, при некоторых или при всех обстоятельствах, под запрещения, содержащиеся в настоящем Протоколе или в каких-либо других нормах международного права, применяемых к Высокой Договаривающейся Стороне.*

Laurent Gisel[1]
International Committee of the Red Cross

How does international humanitarian law constrain cyber warfare and protect civilians?

Scientists, businesses and governments continuously endeavour to invent and develop new technologies, which have the potential to bring about huge benefits for humankind in the economic and social realm. Technological developments in the information and communication field — and in particular the creation and expansion of cyber space which is one of the last decades' defining technological developments — are no exception in that regard. But new technologies also bring about new risks and potential concerns in various realms, in particular if used during armed conflict.

The first time that States placed limits on the choice of means of warfare by way of an international treaty was in the 1868 St Petersburg Declaration, by which they agreed upon '*technical limits at which the necessities of war ought to yield to the requirements of humanity*' and envisaged the possibility to come to subsequent understandings '*in view of future improvements which science may effect in the armament of troops, in order* (...) *to conciliate the necessities of war with the laws of humanity*.' In the spirit of the important principles embodied by the Declaration and in keeping with its own mandate, the ICRC monitors the development of new technologies and their use or potential use in armed conflicts, such as armed drones, autonomous weapons systems or, precisely, cyber warfare. It aims at assessing their actual or potential human cost and analyses how the rules of IHL govern their use. Applying pre-existing legal rules to a new technology also raises the question of whether the rules are sufficiently clear in light of the technology's specific characteristics and foreseeable humanitarian impact.

Businesses, media and governments regularly report that their web-sites or networks have been subject to cyber attacks. However, there is no authoritative definition of the notions of "cyber attack" or "cyber warfare", and they have been used by different people to mean different things. A large proportion of operations referred to as "cyber attacks" constitute illicit information gathering — such as

[1] The views expressed in this article are those of the author alone and do not necessarily reflect the views of the ICRC.

industrial espionage — or other cyber crimes and occur outside the context of armed conflicts. They are not governed by international humanitarian law (IHL). "Cyber warfare" is used in this article to refer to means and methods of warfare that consist of operations against or via a computer or a computer network through a data stream, when such cyber operations are conducted in the context of an armed conflict within the meaning of IHL[2]. Media and commentators also often refer to "information war". Information war is defined notably in the *Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Co-operation in the Field of International information Security*[3], while the U.S. provides a definition of information operations[4]. Though definitions vary and may reflect substantive differences in the understanding of these notions, it seems that information war and information operations are broader notions than cyber warfare as defined here, and often encompass at least part thereof.

The ICRC is particularly concerned by cyber warfare because of the vulnerability of cyber networks and the potential human cost of cyber attacks. If the networks of a State are attacked, civilians risk being deprived of basic essentials such as drinking water, medical care and electricity. If GPS systems are paralysed, there may

---

[2] See ICRC 'How is the Term «Armed Conflict» Defined in International Humanitarian Law?', Opinion paper, March 2008, available at http://www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf.

[3] Annex 1 List of basic terms in the field of international information security: "*Information War — confrontation between two or more states in the information space aimed at damaging information systems, processes and resources, critical and other structures, undermining political, economic and social systems, mass psychologic brainwashing to destabilize society and states, as well as to force the state to taking decisions in the interest of an opposing party*". Unofficial translation available at http://media.npr.org/assets/news/2010/09/23/cyber_treaty.pdf (all web-sites last accessed on 16 June 2014).

[4] 'Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02' (As Amended Through 15 March 2014): "*information operations — The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.*" Available at http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (p. 127). The 2006 version of the DoD 'Joint Publication 3-13, Information Operations' (superseded by the 2012 version) provided a more detailed definition: "*information operations. The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own.*" Available at: http://www.globalsecurity.org/intell/library/policy/dod/joint/jp3_13_2006.pdf (p. GL–9).

be a risk of civilian casualties occurring — for example, through disruption to the flight operations of rescue helicopters that save lives. While the military potential of cyber space is not yet fully understood, experts seem to agree that attacks against transportation systems and electricity networks, or even against dams or nuclear plants are technically possible. Such attacks could have wide-reaching consequences for the well-being, health and lives of hundreds of thousands of people.

It is the role of the ICRC to recall that in an armed conflict, constant care must be taken to spare civilians and civilian objects. Indeed, cyber warfare is subject to IHL in the same way that any new weapons, means and methods of warfare are. There is no legal vacuum in cyber space. This is unambiguously stated in the 2013 report of the United Nations Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security which asserted that "*International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment*"[5]. The Russian Ministry of Defence 2011 *Conceptual views on the activities of the Armed Forces of the Russian Federation in the information space* more specifically stated that the Armed Forces of the Russian Federation have to follow the regulations of IHL during their operations in the information space[6]. An increasing number of States, such as Australia, Canada, Japan, the Netherlands, the U.K and the U.S., or international organisations, such as the European Union, have similarly recognised that IHL applies to cyber warfare[7]. The cardinal principle of the conduct of hostilities under IHL is the obligation to direct attacks against com-

---

[5] 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Note by the Secretary-General', 24 June 2013, A/68/98, p. 8, para 19.

[6] Available at: http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle; (unofficial translation available at http://www.ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf).

[7] Australia: A/66/152, p. 6, last para.; see also: http://foreignminister.gov.au/speeches/2013/jb_sp_131017.html. Canada: A/68/156/Add.1, p. 4, pt. 2. Japan: A/68/156/Add.1, p. 15, first para. The Netherlands: http://cms.webbeat.net/ContentSuite/upload/cav/doc/advies_22_reg_reactie_EN.pdf, p. 5. The U.K.: A/59/116, p. 11, para. 3 and A/65/154, p. 15, para. 7. The U.S.: A/59/116/Add.1 p. 4, para. 5 and A/66/152 pp. 18-19; see also http://www.state.gov/s/l/releases/remarks/197924.htm. The European Union: E.U. Council Conclusions, General Affairs Council meeting, 25 June 2013, 12109/13, p. 4 para. 6 (available at http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2012109%202013%20INIT).

batants and military objectives only. Attacks against civilians and civilian objects are prohibited, and this prohibition also governs cyber attacks. In recent years, there has been increasing concern for the protection of critical infrastructures against cyber attacks. During armed conflict, such attacks would most often constitute violations of IHL. Indeed, drinking water and electricity networks that serve the civilian population, banks, railway networks and public health infrastructure are civilian objects in the first place (at least as long as they have not become so-called "dual-use" objects). As such, they are protected against direct attack. Water systems, in particular, enjoy special protection for being objects indispensable to the survival of the population[8]. Similarly, dams and civilian nuclear plants usually do not fall within the definition of what constitutes a military objective[9], and are thus protected against direct attacks. Even if they become military objectives in particular circumstances, IHL might nevertheless prohibit their attack[10] or at least require that the party to the conflict which would attack them takes particular care to avoid the release of dangerous forces and consequent severe losses among the civilian population[11].

However, to reaffirm the relevance of IHL for cyber warfare and recall such fundamental rules is only the first step. Indeed, cyber warfare raises a number of challenges for the interpretation and application of IHL[12].

First: anonymity. Anonymity in cyberspace is easy to achieve, and this complicates the ability of States to attribute aggressive

---

[8] Art. 54 of the 1977 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocols I) of 8 June 1977 (hereinafter AP I), and ICRC, 'Customary International Humanitarian Law, Vol. I: Rules', Jean-Marie Henckaerts and Louise Doswald-Beck (eds), Cambridge University Press, Cambridge, 2005 (hereinafter ICRC Customary Law Study), Rule 54 (available at: http://www.icrc.org/customary-ihl/eng/docs/v1_rul).

[9] Art. 52 AP I and Rule 8, ICRC Customary Law Study, "*In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose partial or total destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage*".

[10] By virtue of the principle of proportionality, or because of Art. 56(1 and 2) AP I.

[11] Art. 56(3) AP I and Rule 42, ICRC Customary Law Study.

[12] A detailed examination of these challenges can be found in Cordula Droege, *Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians* in The International Review of the Red Cross, Volume 94, nb 886, summer 2012, pp. 533 — 578 (available at: http://www.icrc.org/eng/assets/files/review/2012/irrc-886-droege.pdf)

activities to the perpetrators, and especially to do so in a timely manner. Since IHL relies on the attribution of responsibility to States and other parties to armed conflict, anonymity creates major challenges. If the perpetrator of a given cyber operation cannot be identified, it is extremely difficult to determine whether IHL is even applicable to the operation. The answer to this challenge might, however, not lie in the legal field alone, but first in the technical field.

Second: do cyber operations amount to a resort to armed force triggering the applicability of IHL? There is no doubt that an armed conflict exists when cyber operations are resorted to in combination with traditional kinetic weapons. However, when the first — and possibly the only — hostile act is a cyber operation, can this amount to an armed conflict? This question is closely related but nevertheless distinct from whether a cyber operation alone could amount to a use of force or an armed attack under the United Nations Charter. Such *jus ad bellum* issues are of crucial importance and thus widely debated. However, issues pertaining to *jus ad bellum* and the question of the scope of application of IHL (*jus in bello*) should not be confused. IHL applies in situations of armed conflicts, whether international or non-international, as defined in the 1949 Geneva Conventions and their 1977 Additional Protocols[13]. In that regard, there seems to be no reason to treat cyber operations that would cause effects similar to those caused by kinetic operations differently than the latter. Beyond such kind of operations, the disruption of critical infrastructure lasting long enough to create severe hardship for the population might also be considered as a resort to armed force triggering the applicability of IHL, in view of IHL's purpose to protect the civilian population against such consequences. The ICRC, however, believes that defining the type of cyber operations that triggers the applicability of IHL in the absence of any kinetic operation will be determined only through future State practice[14].

Third: in situations where IHL applies, such as when an armed conflict is already being waged through traditional kinetic means,

---

[13] See ICRC 'How is the Term «Armed Conflict» Defined in International Humanitarian Law?', note 1 above.

[14] ICRC, 'International Humanitarian Law and the challenges of contemporary armed conflicts', 31st International Conference of the Red Cross and Red Crescent, Geneva, 28 November–1 December 2011, Report prepared by the ICRC, October 2011, 31IC/11/5.1.2, p. 37, para. 4, available at http://www.icrc.org/eng/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf

the question arises as to the definition of "cyber attack". The notion of "attack" is cardinal for the rules on the conduct of hostilities in particular for the principles of distinction, proportionality and precautions in attack. Indeed, while parties to a conflict have to take constant care to spare civilians in all military operations and to protect them against the effect of hostilities, most specific obligations governing the conduct of hostilities apply to "attacks". The 1977 First Additional Protocol defines attacks as "acts of violence against the adversary, whether in offence of in defence" (Art. 49(1)). The group of experts which drafted the *Tallinn Manual on the International Law Applicable to Cyber Warfare* defined a "cyber attack" under IHL as "*a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.*"[15] The crux of the matter, however, lies in the detail, namely what is "damage" in the cyber world. A number of IHL experts agree that the loss of functionality of an object may also constitute damage, while others argue that only physical damage is relevant. The ICRC considers that if an object is disabled, it is immaterial whether this occurred through destruction or in any other way[16]. This issue is very important in practice, as a more restrictive view of the notion of attack might imply that fewer and less precise IHL rules would govern and thus restrict such types of operations. In particular, a cyber operation aimed at making a civilian network dysfunctional might not be covered by the IHL prohibition of directing attacks against civilian

[15] Tallinn Manual, Rule 30, p. 106, Available at http://ccdcoe.org/tallinn-manual.html. The Tallinn Manual was drafted at the invitation of the NATO Cooperative Cyber Defense Centre of Excellence. However, the Tallinn Manual is not a NATO doctrine but a non-binding document prepared by a group of experts in their personal capacity. Some have expressed a negative opinion of the Tallinn Manual because it was a regional endeavour and because it would legitimize cyber warfare or promote the militarization of cyber space. This is certainly not the reason for which the ICRC took part as an observer in the group of experts that drafted it. The aim of the ICRC's participation was to ensure that the Manual would uphold the protection that IHL gives to victims of armed conflicts. The ICRC generally agrees with the formulation of the *jus in bello* rules stated in the part of the Manual on "the law of cyber armed conflicts". However, there are exceptions, where the ICRC considers that the norms under existing IHL are actually stronger or more protective than the rules as drafted in the Manual. For more details, see ICRC, 'What limits does the law of war impose on cyber attacks? Questions and Answers', 28 June 2013, available at http://www.icrc.org/eng/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm.

[16] ICRC, 'Report on International Humanitarian Law and the challenges of contemporary armed conflicts', note 13 above, p. 37, last para.

persons and objects under an overly restrictive understanding of the notion of attack.

Fourth: the challenges that the interconnectedness of cyber space creates for the rules of IHL aiming at the protection of civilians and civilian objects. There is only one cyber space, and the same networks, routes and cables are shared by civilian and military users. As the U.K. noted last year, "*[t]he interconnected nature of cyberspace means that disruptive activities against one system may cause unintended and unpredictable effects in other systems*"[17]. The interconnectedness of cyber space might even make it impossible to distinguish between military and civilian computer networks when launching a cyber attack; if carried out nevertheless, such an attack would violate the prohibition of indiscriminate attacks. The use of malware which replicates itself without control and damages civilian cyber networks is similarly forbidden. For example, a party to a conflict would violate the prohibition of indiscriminate attacks under IHL if it releases via the internet a malware tailored to block enemy military radars, while expecting that the malware's code will spread to and affect civilian air traffic control radars. Under the principle of proportionality, a party to a conflict must also do everything feasible to assess whether an attack may be expected to cause incidental harm which would be excessive in relation to the direct and concrete military advantage anticipated, and if that is the case, not conduct the attack. Furthermore, when launching an attack, parties to the conflict have to take all feasible precautions to avoid or at least minimize incidental civilian casualties and damage to civilian objects, including civilian cyber infrastructure and networks. The interconnectedness of cyber space entails the risk that cyber attacks cause incidental damage indirectly. Such indirect incidental damage, however remote it is, has to be considered to the extent that it can be expected — and parties to the conflict that plan or launch cyber attacks have to expect that they risk causing incidental damage indirectly. One could even question whether it is always possible to appropriately assess such indirect effects.

This is just a brief overview of the issue, and there are many other challenges. Some of them reflect challenges that exist for kinetic operations, such as for the definition of the notion of direct participation in hostilities. If someone takes a direct part in hostilities by way of a cyber attack in support of one party to an armed

[17] 'Development in the field of information and telecommunications in the context of international security, Report of the Secretary General', A/68/156 p. 16, para. 1 (response from the U.K).

conflict, he cannot expect the enemy to remain idle. This person would lose his or her legal protection against direct attack, including kinetic attacks, during the execution of the cyber attack and the preparatory measures forming an integral part thereof. Other challenges are possibly more specific to cyber warfare, such as the geography of cyber conflicts, the application of the law of neutrality and the concept of sovereignty, or the definition and legal review of cyber weapons, just to name a few.

Despite these challenges, the key question is not whether new technologies are inherently good or bad. New technologies might also have positive effects if used in a law-abiding manner. In terms of the ability to avoid or minimize incidental civilian harm, precision guided munitions constitute an improvement over artillery or aerial bombardment weapons used during World War II. Without underestimating the challenges, one cannot rule out the possibility that technological evolution might lead in the future to the development of cyber weapons that would, in specific circumstances, cause fewer casualties and less incidental damage than traditional weapons, to achieve the same military advantage. For instance, it might be less damaging to disrupt through a cyber operation certain public services simultaneously used for military and civilian purposes than to destroy such infrastructure through bombardment. In such cases, the principle of precaution arguably imposes an obligation on parties to armed conflicts to choose, whenever feasible, the means least harmful to civilians to achieve their military aim. This being said, a holistic reflection is warranted to fully consider the risks and implications of the use of new technologies from all perspectives and the ICRC is urging States to consider them well before they develop such technologies. While the relevance of IHL as the main body of law that constrains cyber warfare and protects civilians needs to be reaffirmed, the ICRC does not want to rule out that there might be a need to develop the law further to ensure that the protection it provides to the civilian population is sufficient. That will have to be determined by States.

In that regard, there is some debate within the international community on the manner to address the challenges raised by cyber warfare and more broadly those related to information security. In 2011, China, Russia, Tajikistan and Uzbekistan submitted to the United Nations Secretary General an *International Code of Conduct for Information Security*[18], co-sponsored by Kazakhstan and Kyr-

[18] Available at http://nz.chineseembassy.org/eng/zgyw/t858978.htm.

gyzstan in 2013[19]. Russia also put forward a *Draft Convention on International Information Security* (*Concept*)[20], and one of Russia's current priorities in the field of international information security is to promote the formulation and adoption by Member States of the United Nations of international regulations concerning the use of principles and standards of international humanitarian law in the use of information and communications technologies[21]. For its part, the U.K. considers that a multilateral instrument to restrict the use of information technologies in armed conflict is unnecessary, notably because the law of armed conflict already govern such use[22]. Several other States expressed themselves on some of the challenges raised by the application and interpretation of international law to cyber warfare[23]. In December 2013, when requesting the Secretary General to establish a new Group of Governmental Experts, the United Nations General Assembly added to the scope of matters to study "*the issues of the use of information and communications technologies in conflicts and how international law applies to the use of information and communications technologies by States*"[24]. While some of these documents and statements are broader in scope than IHL, the ICRC welcomes the interest given to these issues and will continue to offer its expertise on how IHL constrains cyber warfare with a view to limit its potential human cost, and on how to best address the challenges it raises.

These challenges however underline the necessity for parties to armed conflicts to be extremely cautious, if and when resorting to cyber attacks, to avoid harm to civilians and civilian networks. These challenges also underscore the importance that States which may develop or acquire cyber warfare capacities — whether for offensive or defensive purposes — assess their lawfulness under IHL, as is necessary for any new weapons or methods of warfare. This

---

[19] See A/68/98, p. 8, para 18.

[20] Available at http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument.

[21] 'Basic principles for State Policy of the Russian Federation in the field of International Information Security to 2020', September 2013 available at http://www.scrf.gov.ru/documents/6/114.html, unofficial translation available at http://www.veleposlanistvorusije.mid.ru/doc/pr_20130916_en.pdf (p. 5, para. 12(d)).

[22] 'Development in the field of information and telecommunications in the context of international security, Report of the Secretary General', A/59/116, p. 11, para. 3 (response from the U.K)

[23] See references in note 6 above.

[24] 'Developments in the field of information and telecommunications in the context of international security', A/RES/68/243, 27 December 2013, OP 4.

is required by Art. 36 of the 1977 First Additional Protocol[25], and is the only way to ensure that armed forces and other government agencies potentially resorting to cyber capabilities during an armed conflict will be able to abide by their obligations under international law. The fact that a growing number of States are developing cyber warfare capabilities only reinforces the urgency of these concerns.

---

[25] Art. 36 AP I — New weapons: *In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.*

Пал Вранге

Стокгольмский центр международного права, Швеция

Международное право и вмешательство в национальное и частное киберпространство

1. Введение

В настоящем докладе (*основанном на статье, которая будет опубликована в конце этого года*) *рассмотрен вопрос о том, что вторжение одного государства в киберпространство другого государства может быть запрещено, даже если оно не признано применением силы, являясь не только нарушением суверенитета, но и нарушением прав человека. Этот вывод сделан с общей точки зрения на основе применения существующих норм международного права.*

2. Киберпространство и международное право

Международное право, в том виде, в котором оно существует в настоящее время, применимо к компьютерным сетям. Как правило, государства также придерживаются такой позиции. Это было подтверждено представительной группой правительственных экспертов ООН, которая в своём докладе ООН в июне 2013 года пришла к следующим выводам:

- 19. Международное право, и в частности Устав Организации Объединенных Наций, применимо...
- 20. Государственный суверенитет и международные нормы и принципы, вытекающие из принципа государственного суверенитета, распространяются на поведение государств в рамках деятельности, связанной с использованием ИКТ, а также на юрисдикцию государств над ИКТ-инфраструктурой на их территории.
- 21. Предпринимаемые государством усилия по обеспечению безопасности ИКТ должны гармонично сочетаться с уважением прав человека и основных свобод, закрепленных во Всеобщей декларации прав человека и других международных инструментах.

Однако до разрешения вопроса ещё далеко. За исключением Будапештской конвенции по киберпреступности и, возможно, некоторых положений Конвенции МСЭ (разработанных

задолго до появления Интернета), по этой теме нет международной конвенции. Из существующих документов вышеупомянутый доклад ООН ближе всех подходит к выражению авторитетного межправительственного мнения. Существует мало примеров *opinio juris*[1], очень мало, если есть, примеров применяемой государствами практики, и никаких решений или отчетов международных судебных или контролирующих органов. Даже принципов не очень много; большинство авторов, которые занимаются аспектами международного права в киберсфере, пишут о международном гуманитарном праве и о применении силы. Одним важным исключением является Таллиннское руководство, подготовленное группой экспертов, приглашенных Центром передового опыта по совместной защите от киберугроз НАТО, и опубликованное в 2013 году. В этом документе профессионально, но не полно и не убедительно рассматриваются аспекты использования Интернета в мирное время.

3. Суверенитет и интервенция в киберпространстве

Как предлагается выше, отправной точкой должен быть суверенитет, которым государства обладают в своём киберпространстве, *mutatis mutandis*[2]. Однако у государств может быть множество причин вести деятельность и в киберпространстве других стран. Некоторые из этих причин как таковые являются законными, например, расследование и противодействие терроризму и преступности. Законность других действий, как разведка или саботаж, является сомнительной. Некоторые такие действия могут представлять собой вооруженное нападение, незаконное вмешательство или юридическое противодействие, в то время как другие действия не представляют собой проблему с правовой точки зрения.

Для многих толкователей ситуация, если деяние не является применением силы, в большей или меньшей степени не является проблемной. Однако, большинство таких деяний как, например, шпионаж, могут представлять собой незаконную интервенцию или вмешательство, и этот вопрос гораздо реже был предметом научных дискуссий. Те немногие авторы, которые толковали конкретно принцип невмешательства, в целом согласны, что он применяется в киберпространстве.

---

[1] Убеждённость в правомерности.

[2] С учётом необходимых изменений.

В соответствии с принципом невмешательства и суверенного равенства государств, применение законов государства может, а осуществление государственной власти не может происходить на территории другого государства без согласия этого государства. Это было очень четко подтверждено в постановлении Верховного суда Канады:

Власть вторгнуться в частную сферу личности и собственности и наложить арест на личные вещи и информацию, является парадигматической для государственного суверенитета. Эти действия могут быть санкционированы только государством территориальной юрисдикции.

Существует разногласие по вопросу, запрещены ли кибервторжения, которые не причиняют длительного вреда. Согласно некоторым авторам, ущерб не имеет значения, в то время как другие считают, что незаконным вмешательством являются только те вторжения, которые причиняют материальный ущерб. Однако последнюю точку зрения трудно понять. В соответствии с Будапештской конвенцией о киберпреступности, криминализован ряд деяний, обычно проводимых в рамках правоохранительной деятельности или кибершпионажа (см. ниже). В том числе незаконный доступ и незаконной перехват, и в Конвенции нет исключений для мероприятий, проводимых агентствами иностранных государств. На самом деле, в рамках работы по подготовке Конвенции было четко оговорено, что Конвенция не позволяет дистанционное экстерриториальное расследование. Таким образом, логично сделать вывод, что общий запрет на вмешательство, в том числе запрет на нарушение территориального суверенитета, применяется также и в киберпространстве.

Однако в некоторых обстоятельствах такие действия могут быть оправданы, даже если они не санкционированы. Государство может противодействовать атакам, исходящим из другого государства, и даже в том случае, когда атака не достигает порога вооруженного нападения или даже использования силы. Так, например, если для вируса Stuxnet можно было бы произвести атрибуцию к какому-либо государству, то Иран мог бы принять контрмеры против этого государства. Кроме контрмер, государства могут также ссылаться на необходимость защиты своих важнейших интересов от значительной и неминуемой опасности.

Некоторые из наиболее известных инцидентов, таких как атаки против Эстонии в 2007 году и против Грузии в

2008 году, было трудно приписать непосредственно какому-либо государству. В принципе, государство может нести ответственность за действия отдельных лиц, если они находятся под руководством или контролем государства. Кроме того, государство обязано «не допустить сознательно, чтобы его территория использовалась для совершения деяний, противоречащих правам других государств» (Дело Международного суда ООН о проливе Корфу). В это обязательство входит осуществление действий по расследованию и преследованию в судебном порядке ответственных лиц, как в сотрудничестве с государством-целью атаки, так и в качестве активных превентивных мер. Утверждается, что если государство, чья территория используется для атак, будучи уведомлено о них, не принимает в духе доброй воли меры по их пресечению, то, по крайней мере, в некоторой степени, оно несет за них ответственность. В любом случае, если государство не в состоянии поддерживать правопорядок в своей части киберпространства, это может побудить другие государства принять меры самопомощи.

4. Шпионаж

Одним из наиболее спорных — и, конечно, преобладающим — видом Интернет-активности является кибершпионаж. Сам по себе сбор информации не является незаконным в соответствии с международным правом. Сейчас он в значительной степени осуществляется через Интернет и не обязательно требует согласия правительства, являющегося целью.

Однако, шпионаж может также включать в себя несанкционированное проникновение в серверы, содержащие личную информацию и секретные данные. Некоторые авторы утверждают, что шпионаж является законным в рамках международного права, и что таким образом нет никаких препятствий для осуществления шпионажа через Интернет. Утверждающие это приводят по сути два аргумента. Они указывают, что, во-первых, нет договора, запрещающего шпионаж. Следовательно, если это действие не запрещено, то оно правомерно. Однако этот аргумент не учитывает, что даже если нет всеобщего запрета шпионажа, запрещены многие более конкретные формы шпионажа. В частности, в соответствии со статьей 41(1) Венской конвенции о дипломатических сношениях, государства взяли на себя обязательство, что сотрудники дипломатических миссий — многие из которых в действительности

являются шпионами — должны соблюдать национальное законодательство государства пребывания. Деятельность других государственных агентов охватывается общим запретом на вмешательство, в том числе запрет на принуждение.

Второй аргумент, приводимый этими авторами, заключается в том, что существует соответствующая норма обычного права, поскольку все государства занимаются подобной деятельностью. Однако этот аргумент основан на полном непонимании того, как формируются положения обычного международного права. (Важно не забывать, что по умолчанию многие категории действий, осуществляемых в ходе шпионажа, являются незаконными, так что бремя доказательства лежит на тех, кто утверждает, что для шпионажа есть исключение). Необходимым условием формирования нормы обычного права является не только государственная практика, но и *opinio juris*[3], юридическое убеждение, что эта практика соответствует закону. Я не знаю ни одного государства, которое бы публично утверждало, что шпионаж во всех его формах является законным. Напротив, государства как правило отрицают (или по крайней мере не хотят признавать) причастность к незаконному шпионажу.

Поэтому я делаю вывод, что шпионаж, который включает в себя несанкционированный доступ к серверам и другим компьютерам в иностранном государстве, в целом представляет собой незаконное нарушение суверенитета этого государства.

5. Права человека

Итак, получение несанкционированного доступа к компьютерам в иностранных государствах, как правило, является незаконным согласно международному праву, но в некоторых случаях может быть оправдано. Однако важно отметить, что права человека не могут быть отчуждены государством, гражданином которого является лицо. Следовательно, если государство А осуществляет обыск на компьютере физического лица в государстве Б, то не имеет значения, запрашивает ли А согласие Б или является ли действие оправданным как контрмера.

Наиболее релевантным из прав человека является свобода информации, которая включена в свободу самовыражения, предусмотренную в статье 19 Всеобщей декларации прав че-

[3] Убежденность в правомерности.

ловека (ВДПЧ) и Международного пакта о гражданских и политических правах (МПГПП). В то время как государство имеет право закрыть свои границы — в том числе границы в киберпространстве — оно все равно должно уважать право «получать и распространять информацию и различные идеи независимо от границ». Таким образом, это право придется принимать во внимание при осуществлении государством любых мероприятий по противодействию терроризму или другим преступлениям, например, при пресечении распространения частных или общедоступных сообщений с компьютера.

Далее, существует право на личную жизнь, которое закреплено в статье 12 ВДПЧ и статье 17 МПГПП. Статья 17 МПГПП предусматривает:

1. Никто не может подвергаться произвольному или незаконному вмешательству в его личную и семейную жизнь, произвольным или незаконным посягательствам на неприкосновенность его жилища или тайну его корреспонденции или незаконным посягательствам на его честь и репутацию.

Это относится и к киберпространству. Вторжение государства в сервер в другой стране может представлять собой не только нарушение суверенитета другого государства, но и нарушение прав человека другим человеком. Статья 17 не запрещает любое вмешательство — оно не должно быть произвольным или незаконным — что предполагает необходимость нахождения баланса.

Можно утверждать, что МПГПП не защищает лиц, которые находятся за пределами территории государства, которое вторгается в их частные сферы. Статья 2(1) МПГПП гласит:

1. Каждое участвующее в настоящем Пакте Государство обязуется уважать и обеспечивать всем находящимся в пределах его территории и под его юрисдикцией лицам права, признаваемые в настоящем Пакте, без какого бы то ни было различия...

Комитет по правам человека подтвердил, что Пакт имеет экстерриториальное применение. В деле Лопес Бургос против Уругвая он постановил, что:

Статья 2(1) Пакта накладывает на государство обязательство уважать и обеспечивать права «всем находящимся в пределах его территории и под его юрисдикцией лицам», но это не означает, что соответствующее государство не может быть привлечено к ответственности за нарушения прав, закрепленных в Пакте, которые его агенты совершают на территории

другого государства, будь то с молчаливого согласия правительства этого государства или противодействуя ему.

Таким образом, даже те действия на чужой территории, которые не нарушают суверенитет иностранного государства, могут быть запрещены, поскольку нарушают права человека.

6. Заключение

При обсуждении кибератак с точки зрения международного права много внимания было уделено порогу использования силы. Кибератаки или вторжения, которые не признаются использованием силы, часто признаются беспроблемными. Однако, как было показано в настоящем докладе, такие вторжения часто представляют собой незаконное нарушение суверенитета другого государства или представляют собой нарушение прав человека.

Однако не совсем ясно, как применительно к этому пространству следует понимать обычные нормы международного права. Как уже было сказано, государства не способствуют уточнению этих вопросов.

Конечно, старые принципы и нормы международного права применяются и к киберпространству. Таким образом, отсутствие новой конвенции, не может служить оправданием того, чтобы не пытаться следовать этим правилам. Однако существует насущная потребность в уточнении этих правил международными органами в виде новых конвенций или менее формальных документов. Мы должны знать, что в киберпространстве означают такие термины как «применение силы», «юрисдикция» или «вмешательство». И мы должны знать, имеют ли правительства право вторгаться в нашу частную жизнь. Толкователи международного права должны играть важную роль в этом процессе.

Pål Wrange
Stockholm Center for Intrernational Law and Justice, Sweden

Intervention in national and private cyberspace and international law

1. Introduction

This presentation (*which is based on an article to be published later this year*) *will argue that an intrusion by a state in foreign national cyberspace may be prohibited even if it does not amount to the use of force, both as a violation of sovereignty and as a violation of human rights. That conclusion is arrived at from the point of view of a generalist through the application of existing international law.*

2. Cyberspace and international law

International law, as it currently exists, applies to computer networks. This is also a position generally taken by states. This was confirmed in a report from a broadly representative group of governmental experts, which concluded i.a. the following in a UN report in June 2013:

'19. International law, and in particular the Charter of the United Nations, is applicable ...

20. State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory.

21. State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments.

Still, the situation is far from clear. With the exception of the Budapest Convention against Cybercrime, and possibly some provisions in the ITU Convention (drafted long before Internet), there is no international convention on the topic. The aforementioned UN report is the closest thing we have to an authoritative intergovernmental opinion. There are very few instances of *opinio juris,* very little, if any, confirmed state practice, and no judgments or reports from international adjudicative or monitoring bodies. There is not even very much doctrine; most writers who have engaged in

international law aspects of cyber sphere have written about international humanitarian law and the use of force. One important exception is the Tallinn Manual, drafted by a group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence and published in 2013, which deals expertly but briefly and not conclusively with some peacetime uses of Internet.

3.Sovereignty and intervention in cyberspace

As implied above, the starting point must be that states exercise sovereignty over their respective cyberspaces, *mutatis mutandis*. However, states may have many reasons to take measures also in foreign cyberspace. Some of these reasons are legitimate as such, like investigations of and responses to terrorism and other crimes. Others may be more dubious, like intelligence or sabotage. Some such acts may constitute armed attacks, illegal intervention, or legal countermeasures, while other acts are legally unproblematic.

For many commentators, if an act does not constitute use of force, it appears to be more or less unproblematic. However, many of these acts, like espionage, may constitute illegal intervention or interference, and that issue has been subject to much less academic debate. Those few writers who have commented specifically on the principle of non-intervention generally agree that the principle applies in cyberspace.

Under the principle of non-intervention and the sovereign equality of states, enforcement of a state's laws may and the exercise of public authority may not take place on another state's territory without that state's consent. This was confirmed in very clear terms in a judgment from Canada's Supreme Court:

The power to invade the private sphere of persons and property, and seize personal items and information, is paradigmatic of state sovereignty. These actions can be authorized only by the territorial state.

There is controversy as to if cyber intrusions that do not create any lasting harm are prohibited. According to some writers, damage is irrelevant, whereas others find that only intrusions that cause material harm constitute illegal interventions. The latter view is difficult to understand, though. Under the Budapest Convention on Cybercrime, a number of acts, commonly conducted as a part of law enforcement or cyber espionage (see below), are criminalized. This includes illegal access and illegal interception, and the Convention contains no exceptions for measures taken by foreign public agencies. In fact, the preparatory works of the Convention clearly spell out that the Convention does not allow remote extraterritorial search. Hence, the logical conclusion is that the general

prohibition of intervention, including the prohibition of infringements on territorial sovereignty, applies also in cyberspace.

Nevertheless, even if unauthorized, under some circumstances such measures may be justified. A state may take countermeasures against attacks from another state, and that applies even if the attack does not reach the threshold of an armed attack or even use of force. So, for instance, if the Stuxnet virus could be attributed to a particular state, then Iran could take countermeasures against that state. In addition to countermeasures, states may also invoke necessity, in order safeguard an essential interest against a grave and imminent peril.

Several of the most famous incidents, like the attacks against Estonia in 2007 and against Georgia in 2008, have been difficult to impute directly to a state. In principle, a state may be responsible for acts carried out by individuals, if these individuals are directed or controlled by a state. Furthermore, a state has the duty 'not to allow knowingly its territory to be used for acts contrary to the rights of other States' (ICJ Corfu Channel Case). That obligation includes the duty to investigate and to prosecute, in cooperation with the target state, as well as a measure of active prevention. It is submitted that if a state whose territory is being used for attacks is being notified and still does not take action in good faith, there is at least some degree of responsibility. At any rate, if a state is unable to police its portion of cyberspace, that might invite other states to take self-help measures.

4. Espionage

One particularly controversial — and surely prevalent -- type of Internet activity is cyber espionage. To collect information is — in and of itself — not illegal under international law. This is now to a large extent carried out over the Internet and does not necessarily need the consent of the target government.

However, espionage may also involve unauthorized intrusion into servers that contain private and secret data. Some writers have argued that espionage is legal under international law and that there is therefore no obstacle to committing espionage over the Internet. Those who make that claim essentially say two arguments. First, they point out that there is no treaty prohibiting espionage. Hence, if it is not prohibited, it must be legal. However, this argument misses the point that even though there is no wholesale prohibition of espionage, many more concrete forms of espionage are prohibited. Under Article 41(1) the Vienna Convention on Diplomatic

Relations, for instance, states have undertaken the obligation that staff of diplomatic missions — many of which are in reality spies — must comply with domestic law in the state where they are being stationed. Other state agents are covered by the general prohibition of intervention, including the prohibition of enforcement.

The second argument provided by these writers is that there is a customary norm to that effect, since all nations engage in such activities. However, this is based on a complete misunderstanding of how customary international law is formed. (Remember that the default position is that a number of types of acts conducted in the course of espionage are illegal, so the burden of proof is on those who claim that there is an exception for espionage.) In order for a customary norm to be formed, there needs to be not only state practice, but also *opinio juris*, a legal conviction that this practice corresponds to the law. I know of no state that has publicly claimed that espionage in all its forms is legal. On the contrary, states generally deny (or at least refuse to admit) being involved in illegal espionage.

I therefore conclude that espionage that involves unauthorized access to servers and other computers in a foreign state generally constitute illegal interventions into the sovereignty of that state.

5. Human rights

So, unauthorized access into computers in foreign states is generally illegal under international law, but may sometimes be justified. However, it is important to note that human rights cannot be disposed of by the state of nationality of the person in question. Hence, if state A conducts a search on the computer of an individual in state B, it is immaterial whether A invokes the consent of B or whether the measure is justified as a countermeasure.

One highly relevant human right is the freedom of information, which is included under the freedom of expression, covered by Article 19 in both the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). While a state has the right to close its borders — including borders in cyberspace — it must still respect the right to 'receive and impart information and ideas of all kinds, regardless of frontiers'. This means that any efforts that a state may take in order to counter terrorism or other crimes, for instance by stopping the dissemination of private or public messages from a computer, will have to take this right into account.

Further, there is the right to privacy, protected under Article 12 of the UDHR and Article 17 of the ICCPR. Article 17 of the ICCPR provides:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

This applies in cyberspace, too. An intrusion by a state into a server in another state may constitute not only a violation of that other state's sovereignty, but also a violation of the human rights of another person. Article 17 does not prohibit all interference — interference shall not be arbitrary or unlawful -- which suggests that a balance needs to be struck.

It may be argued that the ICCPR does not protect individuals who are situated beyond the territory of a state which invades their private spheres. Article 2(1) of the ICCPR reads:

Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind...

The Human Rights Committee has confirmed that the convention has extraterritorial application. In the case L pez Burgos v Uruguay, it held that

Article 2 (1) of the Covenant places an obligation upon a State party to respect and to ensure rights 'to all individuals within its territory and subject to its jurisdiction', but it does not imply that the State party concerned cannot be held accountable for violations of rights under the Covenant which its agents commit upon the territory of another State, whether with the acquiescence of the Government of that State or in opposition to it.

Therefore, even measures on foreign soil which do not violate the sovereignty of a foreign state may be prohibited because they violate the human rights of an individual.

6. Conclusion

In international law discourse on cyber attacks, there has been much focus on the threshold for the use of force. Cyber attacks or intrusions which do not amount to the use of force, have often been held to be unproblematic. As I have argued here, however, such intrusions will often constitute illegal interventions into the sovereignty of another state, or constitute violations of human rights.

Nevertheless, it is not completely clear how the usual rules of international law should be understood in this space. As mentioned, states have not been very helpful in clarifying these issues.

For sure, the old principles and rules of international law apply to cyberspace, too. The lack of a new convention is therefore not an excuse for not trying to comply with these rules. Nevertheless, there is a pressing need for international bodies to clarify these rules, in the form of new conventions or less formal documents. We need to know of what terms like 'use of force', 'jurisdiction' or 'intervention' mean in cyberspace. And we need to know if governments may invade our privacy. In that process, commentators on international law should play an important role.

Санджай Гоел
Университет Олбани, SUNY, США

Адаптация международного права к конфликтам в киберпространстве

Добрый день! Прежде всего, я хотел бы поблагодарить Институт проблем информационной безопасности за приглашение на эту конференцию. С момента ее создания я ежегодно принимаю в ней участие, и для меня всегда честь и удовольствие быть здесь. Прежде чем я начну свое выступление, я хотел бы подчеркнуть, что я выражаю не точку зрения правительства США, а свою собственную точку зрения как ученого. Особенно в это время потрясений, когда отношения между США и Россией находятся на низком уровне, мы, как ученые, должны работать более усердно, чтобы гарантировать, что прогресс, которого мы достигли в совместной работе в области киберконфликтов и кибербезопасности, продолжит движение вперёд. Сегодня я хотел бы сгладить негативный образ США — как ученый, я искренне верю, что для Соединенных Штатов важно создать консенсус по вопросу международной кибербезопасности. Несмотря на кратковременные неудачи, долгосрочный прогноз выглядит многообещающим.

Моё выступление сегодня будет посвящено вопросу адаптации международного права к инцидентам в киберпространстве. Я не являюсь ни адвокатом, ни политологом. Мои наблюдения являются попыткой понять, как возможно осуществить адаптацию существующих международных законов к конфликтам в киберпространстве с технической и стратегической точки зрения.

Было предпринято несколько попыток выработать международные соглашения по борьбе с киберпреступностью и для регламентации киберконфликтов. Несмотря на это, прийти к консенсусу по вопросу создания международных законов для киберпространства оказалось трудно. В каждом государстве имеется своя правовая система с различными законами, а законы каждого государства основаны на общественных ценностях, политическом истеблишменте и социальных нормах, сформированных в ходе многовековой истории. Понадобилось много лет для достижения консенсуса по вопросам меж-

дународного права и эти законы, как правило, были приняты после ужасных событий, которые вывели на первый план мировую сознательность. Мы не видели ничего подобного в киберпространстве, и в этом и заключается причина бездействия. Политические лидеры не хотят осознать новые реалии глобализации и изменить политику и законы для решения соответствующих проблем. Это происходит главным образом потому, что эффективное решение этих проблем предполагает гармонизацию законов во всех странах за счет сограждан. Другая причина заключается в том, что, вместо стремления к подлинному компромиссу, страны продолжают демонстрировать жесткую позицию, пытаясь навязать другим странам свои собственные взгляды.

Некоторые ученые утверждают, что киберпространство не отличается от физического, и что существующие международные законы должны применяться к киберпространству. Действительно, между киберконфликтом и другими формами борьбы можно найти много аналогий, и те же принципы, которые применяются к войне в физическом пространстве, могут также применяться для кибервойны. Следовательно, правила обычной войны также применимы к киберпространству. Однако киберпространство обладает достаточным числом отличий, чтобы в некоторых случаях применение этих законов было невозможным. Я уверен, что мы должны взять за основу существующие законы, но при составлении новых международных законов основательно продумать вопросы, связанные с киберпространством.

Далее приведён анализ существующих законов, касающихся международных конфликтов, и выделены ключевые проблемы, возникшие при оценке возможности адаптации существующих законов к киберпространству.

Правила ведения войны

Правила ведения войны развивались через ряд соглашений и имеют несколько положений:

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

Что является законной властью в отношении кибервойны? Кибервойна является тайной войной, и, как правило, осуществляется через прокси-государства — являются ли они легитимными посредниками национальных государств? Согласятся ли когда-нибудь национальные 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)

Во время кибервойны, при проведении контратаки, важна безотлагательность. 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, осуществление которой в случае с киберпространством зачастую требует много времени. В связи с необходимостью мгновенной реакции, во многих случаях пропорциональность трудно обеспечить.

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

Принимая во внимание невозможность однозначной атрибуции, дипломатический спор может быть утомительным и затяжным, в то время как потребность в ответных действиях по отражению атаки (и возможном нанесении при этом побочного ущерба) носит безотлагательный характер.

Право нейтралитета

Это право заключается в том, что нейтральные страны не должны позволять, чтобы их ресурсы были использованы одним государством для нападения на другое государство. Основная проблема здесь заключается в слабости киберинфраструктуры государств. Компьютеры могут быть взломаны для проведения атаки, при этом нейтральные страны могут оставаться в неведении. Можем ли мы возложить на эти страны ответственность за нападения, осуществленные другими государствами, особенно в том случае, если нейтральная страна не имеет технической возможности или ресурсов для обеспечения безопасности своих сетей и защиты от такой деятельности.

Гуманитарное право

Особое внимание уделяется применимости международного гуманитарного права (МГП) к конфликтам в киберпространстве. МГП определяет набор правил, ограничивающих последствия вооруженного конфликта (ПВК), 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 аргументами можно согласиться, необходимо признать, что, в сравнении с физическим пространством, киберпространство обладает отличительными особенностями.

Важно также отметить, что интерпретация законов зависит от точки зрения толкователя. Они могут быть применены неправильно, использованы в узких интересах или отвергнуты по надуманным основаниям. Законы должны быть однозначными и поддающимися исполнению. Для того, чтобы скрыть свою личность, нападающие могут использовать анонимность, которую обеспечивает Интернет. В этом заключается трудность в обеспечении соблюдения правил. Есть несколько явных факторов, которые мешают решению проблемы исполнимости законов и проблемы неоднозначности.

Неоднозначность

Начало гармонизации законов предполагает создание общих однозначных определений используемых государствами терминов. Например, часто обсуждались различия между киберпреступностью, кибервойной и кибертерроризмом. Мы можем добавить сюда еще один термин, то есть киберактивизм. Для всех них инструменты и техника являются общими, разница заключается в акторах и мотивах этих атак. Кибервойна подходит для описания ситуации, когда участие принимают государственные субъекты, а их мотивацией является достижение политических целей. Таким образом, средства ведения кибервойны становятся в арсенале стран еще одним видом оружия, которое может быть использовано в конфликтах. Например, атаки типа «отказ в обслуживании» (DDoS) в последнее время широко используются в кинетических операциях, в основном для психологического воздействия и пропаганды. Когда негосударственные субъекты предпринимают попытки вызвать политические изменения, используется термин «кибертерроризмом» — например, когда Аль-Каида пытает-

ся повлиять на молодых мусульман в Соединенных Штатах, чтобы они присоединились к джихаду. Кибератывизм происходит, когда социальные группы совершают атаки с целью привлечь внимание к социальным и политическим вопросам как внутри одной страны, так и ряда государств. Например, активисты в странах Ближнего Востока ведут кампанию в социальных сетях для политических перемен, а группы хакеров атакуют организации, поддержавшие судебное преследование Джулиана Ассанжа.

Фундаментальная проблема таких определений кроется в различии восприятия. Во-первых, различия между государственными и негосударственными структурами часто размыты, так как негосударственные субъекты зачастую обладают негласной финансовой поддержкой, а также покровительством государственных организаций. Деятельность неправительственных групп связывали с правительствами Ирана, России и Китая. По причине неопределенности, эту взаимосвязь очень трудно убедительно доказать. Во-вторых, определение терроризма, основанное на восприятии разных стран, отличается в этих странах — общественный деятель в одной стране может быть террористом в другой, таким образом, разграничение становится ещё более сложным.

Мотив

По мере того, как спецслужбы и вооруженные силы государств все чаще ведут в киберпространстве шпионаж и подрывную деятельность против других государств, различия между деятельностью в киберпространстве и кибервойной размываются. Руководству государств сложно определить, являются нападения на веб-сайты или хищение данных в Интернете действиями отдельных лиц в другом государстве (руководствующихся мотивами финансовой выгоды, политической или религиозной идеологией) или действиями разведки или вооруженных сил другого государства. Принимая это во внимание, по причине неопределенности мотивов, становится очень трудно отличить потенциальные акты кибервойны от киберпреступности.

Атрибуция

Одной из самых больших проблем обеспечения соблюдения правил кибервойны является атрибуция. Можем ли мы

для применения норм международного права однозначно идентифицировать лиц, совершивших преступления. Есть три категории проблем атрибуции. Первая связана с атаками через Интернет, которые печально известны отсутствием атрибуции. Благодаря архитектуре Интернета, эти атаки могут быть замаскированы, что позволяет злоумышленникам, используя бреши в безопасности многих хост-компьютеров, совершать атаки на компьютеры третьих стран дистанционно. Высокий уровень уверенности в атрибуции едва ли возможен без надлежащего трансграничного сотрудничества или наблюдения. Вторая проблема заключается в нападении на защищенные системы с помощью других носителей, таких как флэш-накопители, компакт-диски и DVD-диски — на иранские ядерные объекты таким образом проник червь Stuxnet. В случае с этими защищенными системами источник нападения должен быть установлен судебной экспертизой и разведкой. Третьей проблемой атрибуции являются предустановленные в аппаратное и программное обеспечение вредоносные программы.

Политическая воля (обзор предпринятых действий)

Было две грандиозных попытки выработать международные законы для киберпространства. В 2001 году Совет Европы (СЕ) принял Конвенцию о киберпреступности[1] (Будапештский договор). Она вступила в силу в 2004 году, однако не была подписана и ратифицирована рядом ключевых стран-членов СЕ, таких как Россия и Турция. Хотя конвенция и открыта для государств, не являющихся членами Совета Европы, и несколько государств её ратифицировали (Австралия, Япония и Соединенные Штаты Америки), в общей сложности к конвенции присоединились только 38[2] из 192 государств-членов Организации Объединенных Наций. Основным предметом разногласий является нежелание стран обеспечить беспрепятственный доступ на свою территорию правоохранительным органам других стран. Интернет не имеет границ, и для того, чтобы правоохранительные органы успешно задерживали, судили и наказывали виновных в транснациональных киберпреступлениях, для отслеживания

[1] Convention on Cybercrime, CETS No.: 185 at: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG

[2] See “chart of signatures and ratifications” at convention webpage above.

преступной деятельности во всей сети Интернет они должны иметь беспрепятственный доступ и не быть скованными государственными юрисдикционными границами. Основанием для беспрепятственного доступа является волатильность данных и задержки при передаче расследования правоохранительным органам других стран. Противники беспрепятственного доступа утверждают, что это является нарушением суверенитета. Трудно в короткие сроки преодолеть недоверие между народами, сформированное многими столетиями конфликтов и широким разнообразием общественных норм. На сегодняшний момент Будапештский договор находится в стагнации и почти не развивается.

В 2011 году Россия представила параллельный договор (концепция Конвенции об обеспечении международной информационной безопасности), в котором акцент сделан на кибервойне. Хотя в нем рассматриваются вопросы кибервойны, он не стал общепринятым из-за геополитики киберпространства. Он превратился в декларацию Шанхайской организации сотрудничества, которая определяет основные принципы ответственного поведения в киберпространстве.

Есть два момента, на которые необходимо обратить внимание:

1. Захочет ли государство поставить себя в невыгодное положение, приняв соглашение об отказе от кибероружия?

2. С циничной точки зрения можно заявить даже то, что законы создаются для слабых стран и не применимы к сильным. Не будут ли благодаря неопределенности атрибуции сильные в военном отношении страны использовать это оружие и отрицать виновность, в то же время выдвигая обвинения против более слабых государств?

Меры укрепления доверия

Целью международного сообщества может стать согласование, подписание и ратификация поддающегося контролю соглашения, которое ограничило бы использование и развитие военных возможностей в киберпространстве — подобно договорам, которые ограничили развитие и распространение ядерного, химического и биологического оружия. Однако, учитывая отсутствие надежных правовых инструментов защиты от кибервойны, и существование трудностей проверки соблюдения договоров, международные организации активно работают над созданием мер укрепления доверия в

киберпространстве. Меры укрепления доверия необходимы для предотвращения нежелательной эскалации инцидентов в результате просчёта, неправильного восприятия, или неверной атрибуции инцидента. Такие меры для киберпространства позволят избежать полномасштабной кибервойны между государствами, и более того, предотвратить развитие безобидного инцидента в войну с применением кинетического оружия.

Существует несколько различных инициатив по разработке мер доверия в киберпространстве. В 2012 году для оценки роли, которую играют меры доверия в обеспечении стабильности киберпространства была проведена конференция ООН. В 2013 году первые многосторонние меры укрепления доверия в области кибербезопасности и безопасности ИКТ были приняты ОБСЕ. Несмотря на то, что они не имеют обязательной силы, они демонстрируют развитие дипломатического диалога по достижению консенсуса в вопросе создания мер доверия. Это чрезвычайно сложная задача.

Меры доверия работают с учётом трех аспектов, а именно, прозрачности, предсказуемости и проверяемости. В то время как в случае ядерного, обычного и химического оружия эти механизмы работали, необходимо оценить их с точки зрения кибервойны. Рассмотрим типичные меры доверия, применяемые в других средах:

1. Передвижения войск и учения
2. Обмен информацией о силах и средствах
3. Обмен специалистами и проведение совместных учений
4. Механизмы экстренной связи для деэскалации ситуации
5. Запрещение применения оружия (например — против критической инфраструктуры)
6. Обучение и образование

Суровая правда заключается в том, что каждая страна стремится занять стратегические позиции для кибервойны. Страны пересматривают свои военные доктрины и включают в них кибервойну как важнейшую сферу противоборства. Стоимость приобретения кибероружия гораздо ниже обычных вооружений. Страны рассматривают кибервойну как способ сбалансировать асимметрию обычных вооружений. В то же время страны, обладающие значительной военной мощью, для поддержания асимметрии вкладывают значительные средства в создание средств нападения и обороны в киберпространстве.

Это приводит к гонке кибероружия. Страны обвиняют друг друга в деятельности, которой они сами занимаются.

Трудно построить доверие в то время как государства стремятся обогнать друг друга в разработке кибероружия. Недоверие, которое осталось со времён холодной войны, и недавние события в Украине не способствуют сотрудничеству.

Было бы печально увидеть, как пропадают даром сформированные за последние 7 лет добрые отношения. Я искренне надеюсь, что мы все сумеем найти общий язык и путь вперёд в текущей геополитической обстановке.

Sanjay Goel
SUNY, USA

Adaptation of International Law to Cyber Conflict

Good Afternoon! I would first like to thank IISI for inviting me to this conference. I have been here each year since its inception and it is always a privilege and a delight to be here. Before I start my remarks, I would like to emphasize that I do not represent the views of the U.S. government, but rather my own views as an academic. Especially at this time of turmoil when U.S. — Russia relations are at a low, we as academics need to work even harder to ensure that the progress that we have made in working together in the areas of cyber conflict and cyber security continues on a path forward. I would like to correct the negative portrayal of United States by this morning — I do sincerely believe from my vantage point as an academic that it is important for the United States to build consensus on the issue of international cyber security and despite short-term setbacks, the long term prognosis is promising.

My remarks today are focused on the adaptation of the international law to cyber incidents. I am neither a lawyer nor a political scientist. My remarks are an attempt at understanding the adaptability of existing international laws to cyber conflicts based on technical and strategic considerations.

There have been several efforts to draw international treaties to address cyber crime and to regulate cyber conflict. However, reaching consensus on creating international laws in cyberspace has been difficult. Each state has a different legal system with diverse laws and each state's laws are based on the societal values, political establishment, and social norms developed through centuries of history. It has taken many years to build consensus on international law and these laws were typically enacted following horrific incidents that brought global consciousness to the fore. We have not seen anything of those proportions in cyberspace and therein lies the reason for the inertia. Political leaders are reluctant to face new realities of globalization by changing policies and laws to address the problems that come with it. This is often because effectively addressing these problems entails harmonizing laws across all countries at the expense of the domestic audience. Another reason is that countries, instead of striving for genuine compromise,

continue to reiterate their intransigent positions while attempting to foist their own views on other countries.

Several scholars have argued that the cyber domain is not distinct from the physical domain and that current international laws should apply to the cyber domain. It is true that there are a lot of analogies between cyber conflict and other forms of warfare and the same principles that apply to physical warfare can apply to cyber warfare. Consequently, the rules of conventional warfare also apply to cyberspace. However there are enough differences in the cyber domain so as to make their enforcement untenable in several cases. I do believe that we need to learn from the existing laws but seriously think through the unique issues of the cyber domain as we build new international laws.

I examine existing laws dealing with international conflicts and raise the key issues while evaluating their adaptation to the cyber domain.

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.

What is a legitimate authority in cyber warfare? Cyber warfare is a covert warfare typically conducted by proxies of countries — are the proxies of nation states legitimate? Would nation states ever agree 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 interest be justified?

3) Need to weigh costs and benefits of involved in waging war (including human life and economic resources)

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

4) Ensure that counter attack be proportional to the violence being encountered

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

5) We must exhaust diplomatic options prior to violence.

With ambiguity in attribution diplomatic wrangling can often be tedious and long drawn while need for response has urgency to repulse the attack (and cause collateral damage).

Law of neutrality

This law asserts that neutral countries should not allow their resource to be used by one country to attack another country. The fundamental problem with this is the weakness of cyber infrastructure of countries. Computers can be infiltrated without cognizance of neutral country to launch attack. Can we hold these countries responsible for the attacks launched by other countries especially if the neutral country does not have technical ability or resources to secure their networks to protect from such activities.

Humanitarian Law

There has been particular emphasis on 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 restricts the means and methods of warfare. While one may agree with the arguments being made, one should recognize the unique difference between the cyber and physical domains. In several instances the citizens of a country are involved in launching.

It is also important to note that laws are subject to interpretation based on ones own point of view. They can be applied erroneously, misused for parochial reasons, or flouted by reasons of reciprocity on flimsy grounds. The laws need to be made such that they are unambiguous and enforceable. The attackers can use the cloak of anonymity that the Internet provides to camouflage their true identities. Therein lies the difficulty in enforcing the rules. There are several explicit factors that make enforceability and ambiguity issues hard to overcome.

Ambiguity

There has to be a common unambiguous definition of terms across the nations as we start harmonizing laws. For instance, there has often been a debate on the distinction between cyber crime, cyber warfare, and cyber terrorism. We can add one more term to this i.e. cyber activism. The tools and techniques are common across

all of these the difference lies in the actors and motivations behind these attacks. Cyber warfare is appropriate when state actors are involved and the motivation is achieve political objectives. Cyber warfare then becomes another weapon in the arsenal of countries that can be used in conflicts. For instance denial of service attacks have been used extensively during recent kinetic warfare incidents mainly for psychological impact and propaganda. When non-state actors are involved in attempting to influence political changes it is termed as cyber terrorism such as Al Qaeda attempting to influence young Muslims in the United States to join the jihad. Cyber activism occurs when social groups launch attacks in order to bring attention to social and political issues both within a country and across multiple countries. For instance activists in middle-east countries campaigning on social media for political change or hacking groups attacking organizations that supported the prosecution of Julian Assange.

The fundamental problem in such definitions is in the differing perceptions. First the distinction between state and non-state actors is often blurred since the non-state actors often have tacit and financial support as well as patronage of government organizations. Non-governmental groups have been linked to governments in Iran, Russia, and China. It is very difficult to prove this nexus conclusively hence this ambiguity. Second the definition of terrorism differs based on perception — a social activist for one country could be a terrorist for another country making the distinctions even fuzzier.

Motive

As the intelligence agencies and militaries of states are increasingly engaging in espionage and subversive activities against other nations in cyber space, distinction between cyber and cyber warfare is blurring. Given that 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, it is very difficult to differentiate potential acts of cyberwar from cybercrime — hence motive is unclear.

Attribution

One of the largest challenges in enforcement of cyber warfare rules is attribution. Can we unambiguously identify the perpetra-

tors of a crime to be able to apply an international law. There are three categories of attribution problems. The first deals with attacks through the Internet which are the most notorious for lack of attribution. These attacks can be camouflaged due to the underlying architecture of the Internet that allows attackers to attack remotely by exploiting lack of security on many hosts allowing them to use machines in a third country for launching attacks. Without proper cooperation across borders 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 such as 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 the malware in the hardware and software that is preloaded.

Political will (Prior Efforts)

There have been two mega efforts in order to create international laws for cyber space. The 2001 Council of Europe (CoE) Convention on Cybercrime[1] (Budapest Treaty) entered into force in 2004, however, it has not been signed and ratified by several key CoE member states such as Russia and Turkey. Although the convention is open to non-CoE member states and several have ratified it (Australia, Japan and the United States), a total of only 38[2] of the 192 member states of the United Nations have acceded to the convention. The main point of contention is the reluctance of countries to provide unfettered access to law enforcement agencies of other countries. The Internet has no borders and in order for law enforcement authorities to successfully apprehend, prosecute and punish perpetrators of transnational cybercrimes, authorities must get unfettered access to track criminal activities across the entire Internet unfettered by states' jurisdictional boundaries. The justification for unfettered access is the volatility of data and delays in handing over investigations to law enforcement authorities of other countries. Opponents of unfettered access argue that it is a violation of sovereignty. The distrust among nations built through centuries of conflict and the wide diversity in societal norms is hard to bridge in a short time. At this point the Budapest Treaty has stagnated with minimal traction. In 2011, Russia released a

[1] Convention on Cybercrime, CETS No.: 185 at: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG

[2] See "chart of signatures and ratifications" at convention webpage above.

parallel treaty (eKaterinburg Treaty) that focuses on cyber warfare. Though it addresses the issues of cyber warfare, it did not have the traction to become universally acceptable because of geopolitics of cyber space. It has been morphed into the Shanghai Cooperative Organization declaration that defines fundamental principles for responsible behaviour in cyber space.

There are two points to note:

1) Would a country like to be handicapped by agreeing to a treaty to not be able to deliver cyber weapons?

2) A cynical view would go so far as to state that the laws are for the weak countries they don't apply to the strong. Would the militarily stronger countries use these weapons and deny culpability while prosecuting the weaker ones based on ambiguity in attribution?

Confidence building measures

the goal of the international community may be to negotiate, sign and ratify a verifiable treaty that would limit the use and development of cyber warfare capabilities, similar to treaties that have limited the development and spread of nuclear, chemical and biological weapons. However, given the absence of credible legal instruments to protect against cyber warfare and difficulty in verifying compliance with treaties, international bodies are working arduously to create Confidence Building Measures (CBMs) in cyber space. The role of CBMs is to prevent unintended escalation of an incident by miscalculation, misperception, or misattribution of an incidence. Such measures for cyberspace would avoid a full-scale cyber war among nations and worse yes prevent precipitation of an innocuous incident into kinetic war.

There are several different efforts underway to develop CBMs in the cyber arena. United Nations held a conference in 2012 to assess the role of Confidence Building Measures to assure stability in cyber space in 2012. OSCE adopted the first ever cyber/ICT security related multilateral confidence-building measure in 2013. While non-binding and innocuous this shows a diplomatic momentum building towards a consensus in creating CBMs. This is going to be an extremely challenging task.

CBMs are aligned along three primary dimensions, i.e., transparency, predictability, and verifiability. While this has worked in other avenues, i.e. nuclear, convention, and chemical warfare it needs to be evaluated for cyber warfare. Let us examine the typical CBMs from other domains.

1) Troop movements and exercises
2) Exchange of Information about assets
3) Exchange of personnel and joint exercises
4) Communication mechanisms to deescalate situations
5) Prohibited Weapons (For instance — critical infrastructure)
6) Training and Education

The hard truth is that each country is engaged in strategically positioning themselves for cyber warfare. Countries are redefining their military doctrines to include cyber warfare as a critical arena of conflict. The cost to acquire cyber weaponry is much lower than that for conventional weapons acquisition. Countries are considering cyber warfare as a way of balancing asymmetry in conventional weaponry. At the same time countries with favourable military strengths are investing heavily in both cyber offense and defence to ensure the continuation of asymmetry — leading to the cyber arms race. Countries are blaming each other for activities that they are themselves engaged in.

It is hard to build confidence at the same time as countries race forward to overtake each other in developing cyber weapons. Distrust lingering on from the cold war and the new developments in Ukraine do not help the cause of cooperation.

It would be such a waste to see all the goodwill that we have built over the last 7 years to go to waste. I sincerely do hope we are all able to find common ground and a way move forward through the current geopolitics.

Сандро Болонья

Итальянская ассоциация экспертов по критически важной инфраструктуре

Кибербезопасность и устойчивость промышленных систем управления

Промышленные системы управления и последствия для безопасности

Средства автоматизации являются важной частью ядра любой технологической инфраструктуры (электрических сетей, нефте- и газопроводов, телекоммуникационных сетей, финансовых систем, и т.д.), и таким образом, для стабильной работы без последствий в случае нападений и инцидентов должна постоянно обеспечиваться их безопасность. Промышленные системы управления и их компоненты применяются для управления в различных инфраструктурах, от энергетики до производства и систем очистки воды, и конечно они необходимы для функционирования инфраструктур, системы которых, как правило, тесно взаимосвязаны и взаимозависимы. Можно прямо сказать, что будучи в состоянии контролировать какую-либо часть промышленных систем управления, можно управлять механизмами всей инфраструктуры. Нет никаких сомнений, что кибератаки на промышленные системы являются наиболее распространенным и наиболее разорительным видом атак [1].

Составление исчерпывающих списков кибератак является трудной задачей, потому что государственные учреждения, национальные критические инфраструктуры, крупные лаборатории и другие подобные структуры, как правило, не стремятся раскрывать факты совершения и обстоятельства кибератак. Среди самых известных и произошедших недавно атак выделяются Stuxnet, Flame и Duqu. Из них только Stuxnet была направлена на причинение ущерба целевой инфраструктуре, а остальные использовались для шпионажа. Действительно, Stuxnet, как полагают, является первой вредоносной программой, целью которой были конкретно системы критически важной инфраструктуры. Считается, чтобы она была разработана для выключения центрифуг на заводе по

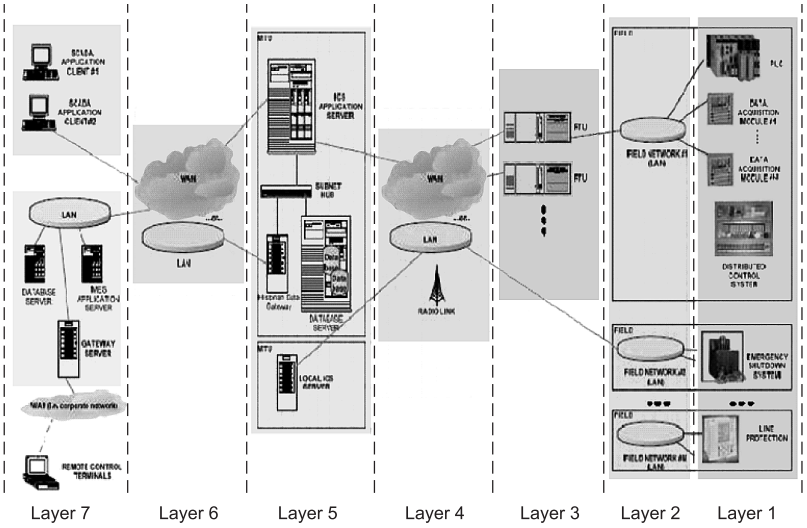
обогащению урана в иранской Натанзе, где, как сообщается, в тот период времени наблюдались остановки и другие проблемы. Этот технически сложный червь распространяется через USB-накопители и четыре ранее неизвестные уязвимости в операционной системе Windows, известные как «уязвимости нулевого дня»[1].

Первоочередные мероприятия противодействия киберугрозам сосредоточены на технической стороне проблемы, и представляют собой вложения в такие меры безопасности как брандмауэры, антивирусы и другие программно-аппаратные решения для обнаружения вторжений. Однако есть понимание, что эта проблема не может быть решена только на техническом и операционном уровне, так как сейчас стало ясно, что многие из вышеупомянутых технических решений неэффективны или их недостаточно в тех случаях, когда они не интегрированы с решениями резервирования. Масштаб проблемы обеспечения безопасности может ввести в ступор, но этого можно избежать. В действительности ответы есть, и в их основе — технологии. Но технологии являются только инструментом. Управление в конечном итоге находится в руках людей. Это означает, что для эффективной защиты от кибератак культура безопасности должна быть на одном уровне со средствами обеспечения безопасности.

Устойчивость, обычно понимаемая как способность инфраструктур или услуг быстро “прийти в норму” после атаки или нейтрализовать её потенциал, в настоящее время считается экономически обоснованной политикой, в дополнение к существующим мерам предупреждения и защиты, которые являются основой существующих программ защиты критических инфраструктур. Этот новый подход становится все более важным, особенно на фоне участившихся за последние годы кибератак, и усиления опасений глобального выхода из строя, нарушения функционирования и общего недоверия ко многим услугам, необходимым современному обществу. Устойчивость является спроектированной способностью, заложенной в защиту и жизненный цикл управления инфраструктурой, что позволяет сложным системам противостоять различного рода атакам или ослаблять их воздействие, и, соответственно, уменьшать последствия, которые существуют, несмотря на созданные в этих системах защитные барьеры [2].

---

[1] http://news.cnet.com/8301-1009_3-57560799-83/stuxnet-attacks-iran-again-reports-say/



Семь слоёв физической архитектуры промышленных систем управления[2]

По этой причине необходимо распространение информации и повышение осведомленности о том, что представляет собой кибербезопасность промышленных систем управления, в том числе понимание важности потенциальных последствий внедрения слабых методов кибербезопасности. Конечно, термин «кибербезопасность» охватывает как преднамеренные нападения извне и изнутри, так и непреднамеренную неправильную эксплуатацию систем.

Здесь очень важно подчеркнуть различие между промышленными системами управления и корпоративными информационными системами. И те, и другие могут быть объектами кибератак, но эти системы различны по своей природе, и поэтому атаки и их последствия также отличаются. Одно из главных отличий заключается в том, что такие операционные системы, как Microsoft Windows или Apple MacOS X общедоступны, и их относительно легко изучить и проанализировать в связи с более широкой аудиторией потребителей и пользователей. Промышленные системы управления совсем другие. Их труднее приобрести, так как они обслуживают ограниченный круг потребителей, в основном промышленные компании, и для того, чтобы выполнить на них атаку, необходимы

[2] S. Bologna, *ICS and Smart Grids Security Standards, Guidelines and Recommendations,* presentation at ERNCIP conference, JRC Ispra, 2012

глубокие практические знания аппаратного и программного обеспечения. Также стоит отметить, что для разных систем существует множество разных производителей и поставщиков. В отличие от кибератак на доступные в свободной продаже операционные системы, например, Windows или Mac OSX, которые (как и их дефекты) широко распространены (так как многие системы и сети зависят от них), нападение на конкретную промышленную систему управления основано на глубоком знании этой системы и её особенностей.

Анализ секторов, подвергшихся кибератакам (2009–2013)

Для выявления динамики кибератак на сектора экономики группой реагирования на компьютерные происшествия промышленных систем управления США (ICS-CERT) было проведено соответствующее исследование, охватившее период 2009–2013 гг.

В 2009 году было зарегистрировано девять инцидентов. Наиболее подвержены атакам были сектор водоснабжения (33,4%) и сектор энергетики (33,3%)[3].

В 2010 г. число зарегистрированных инцидентов увеличилось до сорока одного. Наиболее подверженным атакам был сектор энергетики с 18 атаками, что составило 44% от общего числа. В 2010 г., в связи с обнаружением Stuxnet, ядерная промышленность вошла в число секторов, подвергшихся нападениям (5,12% от общего числа)[4].

В конце 2011 г. количество сообщений о случаях атак резко возросло до 198, из них 81,41% пришлось на сектор водоснабжения, остальные — на сектор энергетики, ядерную промышленность, государственные учреждения и сектор химической промышленности[5].

Удивительно, но согласно Операционному докладу ICS-CERT за 2012 финансовый год (октябрь 2011г. — сентябрь 2012г.), число зарегистрированных нападений почти такое же, как и в 2011 году, но с другим лидирующим по количеству нападений сектором — это энергетика с 41% от общего числа зарегистрированных случаев[6].

---

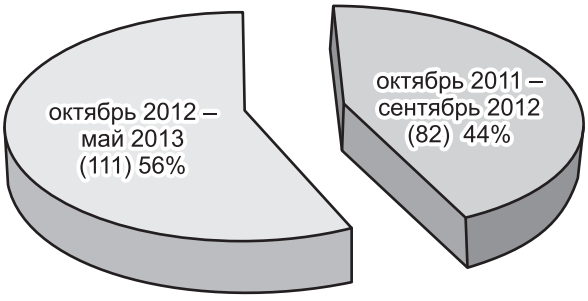
[3] ICS –CERT Incident Response Summary Report 2009-2011, available from: https://ics-cert.us-cert.gov/sites/default/files/documents/ICS-CERT%20Incident%20Response%20Summary%20Report%20(2009-2011)_accessible.pdf

[4] *Ibidem.*

[5] *Ibidem.*

[6] ICS-CERT Monthly Monitor Oct-Dec 2012, available from: http://ics-cert.us-cert.gov/pdf/ICS-CERT_Monthly_Monitor_Oct-Dec2012.pdf

Зарегистрированные инциденты по секторам (2012 г.)



Согласно Операционному докладу ICS-CERT за первую половину 2013 года (октябрь 2012 — май 2013), число зарегистрированных нападений по-прежнему увеличивается. Наиболее атакуемым сектором по-прежнему является энергетика, на которую приходится 53% от общего числа атак.

Энергетика — наиболее часто атакуемый сектор

Принимая во внимание, что вышеприведенный анализ охватывает только отчеты о кибератаках на критическую инфраструктуру США, это не позволяет сделать какие-либо общие выводы. Однако важно отметить то, как значительно с 2010 года возросло количество инцидентов, связанных с кибератаками, а также число секторов, подвергшихся кибератакам.

Общие уязвимости и методы атак

Уязвимости

Быстро обосновать причины, по которым операторам киберинфраструктур (или инфраструктур, зависящих от ИКТ-систем) следует уделить больше внимания проблеме устойчивости, можно, если принять во внимание все «известные» уязвимости и методы нападения, которые могут негативно повлиять на жизненный цикл киберсистем (и работу зависящих от этих систем услуг).

Наиболее часто возникающие уязвимости и атаки кратко обобщены в последующих списках [3]:

Уязвимости

- Присущие программному/аппаратному обеспечению уязвимости (недостатки конструкции).
- Отсутствие (физических и логических) мер защиты.
- «Уязвимости нулевого дня».
- Неправильная конфигурация / несовместимость компонентов системы.
- Отсутствие обновлений или ненадлежащее тестирование обновлений перед установкой/внедрением.
- Недостаточная подготовка системных администраторов.
- Недостаточное обучение пользователей.
- Устаревание инфраструктуры или частей систем.
- Недостатки корпоративной политики в области информационных технологий (удостоверения личности продолжают быть действительными даже после ухода на пенсию/перевода/увольнения работников).
- Недооценка рисков, являющихся следствием физической уязвимости объектов, в которых размещены киберсистемы (например, подверженность затоплению, злоумышленным действиям, и т.д.).

Атаки

- Распределенный отказ в обслуживании (DDoS);
- Сетевые вторжения;
- Вредоносное программное обеспечение, троянские кони, бэкдоры;
- Атаки на определенных пользователей (администраторов — операторов на ключевых позициях);
- Атаки на определенное оборудование/устройства (например, программируемые логические контроллеры — PLC);

- Полное или частичное разрушение систем (по причине, например, пожара, взрыва и т.п.);
- Социальная инженерия;
- Инсайдеры.

Важность (и способность нанести вред киберсистемам) обеих вышеупомянутых категорий возросла в связи с массовым внедрением технологий во всех корпоративных и государственных секторах, а также по причине быстрого развития рыночной конкуренции — обстоятельство, которое в некоторых случаях заставляет поставщиков технологий продавать не полностью протестированное оборудование.

Можно утверждать, что развитие устойчивости, так же как и внедрение защиты, обосновано давно известными переменными и осознанием того, что без защиты нет устойчивости, и наоборот.

В то же время важно подчеркнуть, что принятие мер устойчивости ни в коем случае не должно отвлекать или снижать внимание к защите, так как эти подходы дополняют друг друга, и должны в равной степени присутствовать в жизненном цикле управления и безопасности современных инфраструктур.

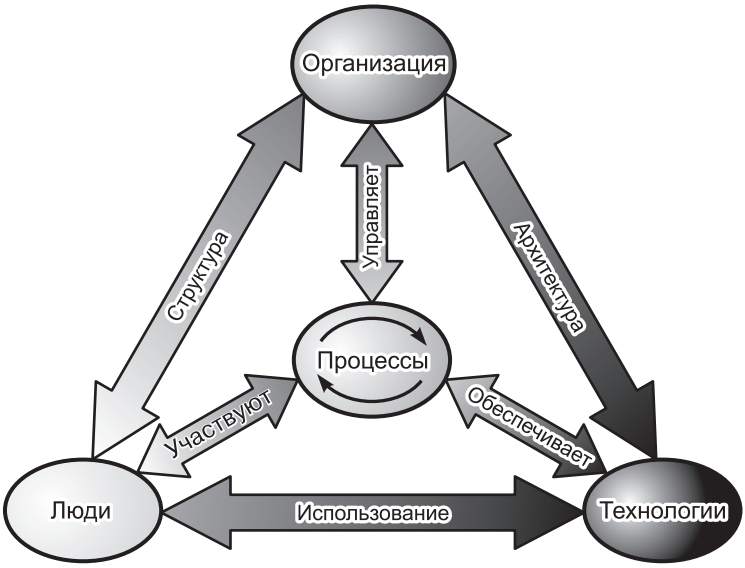
Подход, ориентированный на устойчивость

Опыт прошедших лет и недавних событий выявил вероятность, когда меры защиты в конце концов могут дать сбой. По этой причине, и учитывая, что меры защиты критически важных инфраструктур можно легко обойти, всем заинтересованным сторонам, участвующим в обеспечении безопасности таких деликатных и жизненно важных объектов инфраструктуры, крайне необходимо уделять больше внимания устойчивости критической инфраструктуры.

Критическая инфраструктура — это не только технологии, но и в большой степени люди, процессы и организации. Для того чтобы процессы анализа рисков и управления рисками были всеобъемлющими и успешными, необходимо принимать во внимание все эти компоненты, а также культурный фон.

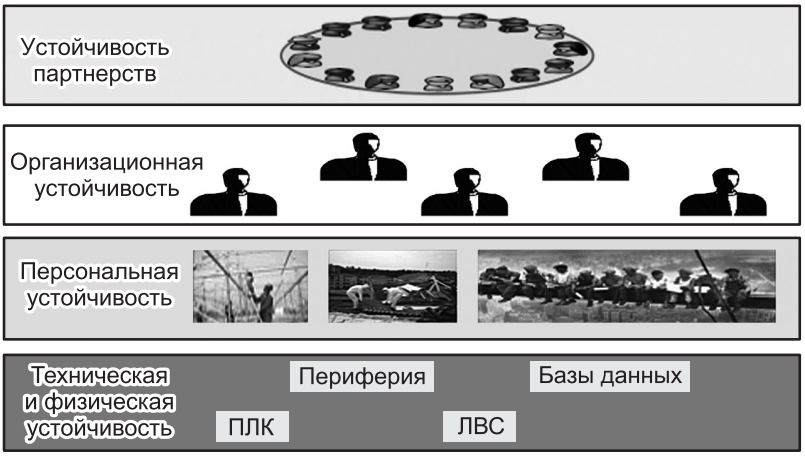
Политика устойчивости киберсистем, создаваемая с нуля, должна основываться на четырех линиях обороны.

Первая линия обороны находится на техническом и физическом уровне. Физическая и техническая устойчивость представляют собой способность критической инфраструктуры, с учетом реализованных защитных механизмов, сдерживать или замедлять противника (заборы, замки и т.д.), регистрировать атаки (охранники, датчики, электронные системы контроля



доступа и т.д.), и/или снижать уязвимость (недостатки или слабые места в системе безопасности). Такие традиционные элементы управления сетевой безопасностью, как межсетевые экраны, системы предотвращения вторжений и антивирусная защита широко распространены и достаточны для противодействия известным угрозам, но недостаточны для снижения риска от неизвестных (например, «уязвимостей нулевого дня»), незаметных (например, отсутствие подготовки или наличие инсайдеров), или угроз, которые не могут быть адекватно учтены (например, ограничения программного/аппаратного обеспечения или устаревание инфраструктуры). Эти традиционные элементы управления сетевой безопасностью зачастую являются основой противодействия продвинутым угрозам, многие из которых имеют доступ к современным научным разработкам. В то время как противник применяет новые идеи, в основе защиты большинства инфраструктур безопасности продолжают использоваться устаревшие технологии [4].

Вторая линия обороны находится на персональном уровне. Персональная устойчивость является одним из важнейших компонентов устойчивости систем. Главным упущением в этом вопросе является не распределение ролей и обязанностей (специфических для каждого работодателя) служащих в случае чрезвычайной ситуации, а персональная устойчивость,



Четыре линии обороны современной устойчивости

которая заключается в личной подготовленности сотрудников. Таким образом, в чрезвычайных ситуациях сотрудники быстрее ориентируются и лучше подготовлены к исполнению специфических функций и обязанностей в конкретной организации. Создание культуры устойчивости уже является насущной необходимостью, которая потребует от организаций изменения восприятия бедствий или чрезвычайных ситуаций. В условиях, когда мир становится все более изменчивым и нестабильным, для организаций одним из наиболее ценных качеств может стать способность быстро приспосабливаться для выживания в непредвиденных чрезвычайных ситуациях [5].

Третья линия обороны находится на организационном уровне. Предполагается, что организационная устойчивость лучше всего достигается путем систематического разделения ее элементов на основе четких критериев. Это позволяет изолировать каждый из компонентов и облегчает выявление их ключевых атрибутов или характеристик. Организационная устойчивость опирается на техническую устойчивость и персональную устойчивость, о которых говорилось выше, а функциональная устойчивость должна представлять собой четкое распределение ответственности и определение, кто и что должен делать [6].

Четвертой линией обороны является развитие сотрудничества и партнерства между различными заинтересованными сторонами. В Европе для развития политической инициативы по защите критически важной информационной инфраструктуры, принятой Европейской комиссией 30 марта 2009 г., было

создано Европейское государственно-частное партнерство для повышения устойчивости (EP3R). Целями EP3R являются: поддержание процесса обмена информацией, накопление передового опыта в области политики и промышленности, развитие общего понимания, обсуждение приоритетов, целей и мероприятий государственной политики, повышение согласованности и координация политики в области безопасности и устойчивости в Европе, выявление хороших базовых практик и содействие их принятию для обеспечения безопасности и устойчивости[1].

Международные подходы к обеспечению устойчивости

7 февраля 2013 была представлена «Стратегия кибербезопасности Европейского Союза: открытое, безопасное и защищенное киберпространство»[2]. Свои комментарии к ней дали Верховный представитель ЕС Кэтрин Эштон[3], вице-президент Европейской комиссии по цифровой повестке дня Нели Крус[4], и комиссар ЕС по внутренним делам Сесилия Мальмстрем[5]. Было отмечено, что необходимость защиты от кибератак предопределяется нашей зависимостью от киберпространства почти в каждом секторе нашей жизни. Нели Крус подчеркнула важность киберустойчивости, как одного из ключевых пунктов Стратегии ЕС: «Мы должны защитить наши сети и системы, и сделать их устойчивыми. Это может произойти только когда все участники процесса будут играть свою роль и выполнять свои обязанности. Киберугрозы не

---

[7] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r

[8] European Commission (2013), *Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyberspace.,* available from: http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/join_2013_1_en.pdf

[9] Remarks by EU high representative Catherine Ashton at the at press conference on the launch of the EU's Cyber Security Strategy, February 7th 2013, available from: http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/EN/foraff/135287.pdf

[10] Neelie Kroes, "*Using cybersecurity to promote European values",* speech at the at press conference on the launch of the EU's Cyber Security Strategy, February 7th 2013, available from: http://europa.eu/rapid/press-release_SPEECH-13-104_en.htm

[11] Cecilia Malmström, "*Stepping up the fight against cybercriminals to secure a free and open Internet",* speech at the at press conference on the launch of the EU's Cyber Security Strategy, February 7th 2013, available from: http://europa.eu/rapid/press-release_SPEECH-13-105_en.htm

сдерживаются национальными границами — так должно быть и с кибербезопасностью. Соответственно, к нашей Стратегии прилагается предложенная Директива по укреплению киберустойчивости в пределах нашего общего рынка. Она обеспечит принятие компаниями мер, необходимых для безопасности и стабильности сетей. [...] Европе нужны устойчивые системы и сети. Бездействие приведёт к значительным затратам у потребителей, предприятий, общества. Ущерб от одного киберинцидента может измеряться десятками тысяч евро для малого бизнеса — и миллионами в случае крупномасштабной утечки данных. Однако большинство из этих инцидентов могли бы предотвратить сами пользователи, применяя простые и не затратные меры»[1].

12 февраля 2013 года президент США Барак Обама подписал правительственное распоряжение о «Совершенствовании кибербезопасности критически важной инфраструктуры»[2]. По содержанию и предложенным мерам этот документ похож на Стратегию кибербезопасности Европейского Союза.

19 марта 2013 в итальянском государственном издании был опубликован долгожданный закон о кибербезопасности[3] (Декрет Председателя Совета Министров от 24 января 2013). Указ устанавливает новую правительственную систему противодействия потенциальным угрозам кибербезопасности в Италии.

Созданную указом организационную структуру возглавляет Премьер-министр, наряду с «Комитетом безопасности Итальянской Республики», задачей которого является определение стратегии национальной безопасности (так называемой «Национальной стратегии кибербезопасности»). Первый уровень организационной структуры поддерживает «орган коллегиальной координации». Во главе органа коллегиальной координации стоит Генеральный директор Департамента информационной безопасности. В заседаниях органа коллегиальной координации также принимает участие военный советник Премьер-министра.

---

[12] Neelie Kroes remarks, op. cit.

[13] Barack Obama, "Improving Critical Infrastructure Cybersecurity" Executive Order of February 12, 2013, available from: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[14] Available at: http://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2013-03-19&atto.codiceRedazionale=13A02504&elenco30giorni=true

В феврале 2014 года были опубликованы «Национальные стратегические основы безопасности киберпространства»[1] и «Национальный план по защите киберпространства и обеспечению безопасности ИКТ»[2].

В «Национальных стратегических основах безопасности киберпространства» изложены стратегические ориентиры, которые должны быть реализованы под руководством Комитета безопасности Республики совместными скоординированными усилиями всех ключевых заинтересованных органов, входящих в систему национальной кибербезопасности, определенную декретом Премьер-министра от 24 января 2013 года.

Это, несомненно, является признаком того, насколько важной задачей становится обеспечение кибербезопасности критических инфраструктур и их систем управления в различных ситуациях.

Использованная литература

[1] Sandro Bologna, Alessandro Fasani, Maurizio Martellini: Cyber Security Deterrence and IT Protection for Critical Infrastructures, SpringerBriefs in Computer Science 2013, pp 57-72

[2] Paul Theron, Sandro Bologna: Critical Information Infrastructure Protection and Resilience in the ICT Sector, Book, IGI Global, 2013.

[3] Sandro Bologna, Stefano Mele, Alessandro Lazari, "Improving Critical Infrastructure Protection and Resilience against Terrorism Cyber Threats", NATO Advanced Research Workshop Managing Terrorism Threats to Critical Infrastructure — Challenges for South Eastern Europe" Belgrade, Serbia, May, 2014.

[4] General Dynamics 2010, Defending against cyber attacks with session-level network security.

[5] Ann Coos, Ronald Bearse, 2013, Strengthening Resilience of the Nation's Most Important Asset: People, The CIP Report, December 2013.

[6] Wayne Boone, 2014, Functional Resilience: The "Business End" of Organizational Resilience, The CIP Report, January 2014.

---

[15] Available at: http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf

[16] Available at: http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-cyber-security-plan.pdf

Dr. Sandro Bologna
Italian Association of Critical Infrastructure Experts

Cyber Security and Resilience of Industrial Control Systems

Industrial Control Systems and Implications for Security

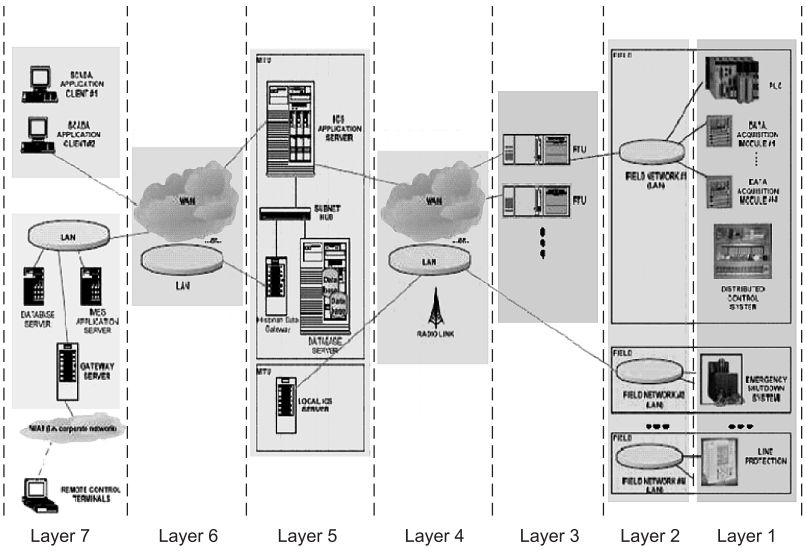
Industrial Control Systems are an important part of the core of any Technological Infrastructure (Electricity Grid, Oil and Gas Transmission Grids, Telecommunication Networks, Financial Systems, etc..) and thus they need to be constantly secured in order to work properly and without consequences in case of attacks and incidents. Industrial Control Systems and their components control different kind of infrastructures, from energy production, to manufacturing and water treatment, and they are obviously critical to the operation of infrastructures that are often highly interconnected and mutually dependent systems. It's straightforward to say that being able to control any part of an Industrial Control System permits the manipulation of the mechanisms of an infrastructure. There is no doubt that cyber attacks are the most common and most costly attacks in Industrial Control Systems [1].

Producing comprehensive lists of cyber attacks is not an easy task because, generally, government agencies, national critical infrastructures, large-scale laboratories and other critical actors do not tend to disclose whether a cyber attack has taken place neither the details of it. Among the most popular and recent, are: Stuxnet, Flame and Duqu. Among these attacks only Stuxnet was aimed to causing damage to the target infrastructure, while the others were used for espionage. Indeed, Stuxnet is believed to be the first malware targeted specifically at critical infrastructure systems. It's thought to have been designed to shut down centrifuges at Iran's Natanz uranium enrichment plant, where stoppages and other problems reportedly occurred around that time. The sophisticated worm spreads via USB drives and through four previously unknown holes, known as zero-day vulnerabilities, in Windows.[1]

The first response against cyber threats has been focused on their technical side, investing in security measures such as firewalls, an-

[1] http://news.cnet.com/8301-1009_3-57560799-83/stuxnet-attacks-iran-again-reports-say/

tivirus and other software/hardware intrusion-detection solutions. However, there is a growing understanding that this problem cannot be dealt on a technical and operational level only, as, nowadays, many of the aforementioned technical solutions have proven to be ineffective or insufficient if not integrated with redundancy-oriented solution. It is easy to get lost on the enormity of a security solution, but it doesn't have to be that way. Yes, there are answers and it starts with technology. But technology ends up being a solid tool. In the end, people wield the power. That means security culture must be on a par with safety effectively protect against cyber attacks.



Seven Layer Physical ICS Architecture[2]

Resilience, commonly intended as the capability of the infrastructures or service to rapidly "bounce back" after an attack or to absorb and frustrate its potential, is now deemed an economically justified policy in complement of existing prevention and protection policies that stand as the pillars of current Critical Infrastructure Protection programs. Such new approach is increasingly important especially since cyber attacks have multiplied in recent years increasing the fear of global digital-breakdowns, deviation of use and general distrust of many services essential to the modern society.

[2] S. Bologna, *ICS and Smart Grids Security Standards, Guidelines and Recommendations,* presentation at ERNCIP conference, JRC Ispra, 2012

Resilience is an engineered aptitude, embedded in the infrastructures' protection and management lifecycle, that allows complex systems to survive to different kind of attacks or to diminish their impacts, and consequently incidents that occur despite defence barriers crafted into those systems [2].

For this reason, it is mandatory that awareness should be raised in the knowledge of what the cyber security of Industrial Control System is, and in this sense, understanding what the potential consequences of adopting a loose cyber security methods could be is pivotal. Of course, the term "cyber security" encompasses both deliberate attacks from the outside and inside, and the unintentional misuse of the systems.

A point that is really important to stress is the difference between an Industrial Control System and a Corporate Information System. Both can be targets of cyber attacks, but they have different nature and so the attacks and the consequences. One of the main differences is that Operating Systems such as Microsoft Windows or Apple Mac OSX are available to anyone and so relatively easy to study and analyze, due to the wider audience of consumers and users. ICS are a different thing. They are more difficult to acquire since they serve a limited scope of consumers, mainly industrials, and in order to perform an attack on those, a deep practical knowledge on both hardware and software is needed; also it is worth mentioning that there are multiple producers and vendors, differencing system from system. In contrast to a cyber attack against retail operating systems that is widespread because many systems and networks depend on them — Windows or Mac OSX, for example — and their flaws, an attack to a specific Industrial Control System is based on a deep knowledge on that specific system, with its own peculiarities.

Analysis of sectors targeted by cyberattacks (2009–2013)

The United States Industrial Control Systems Cyber Emergency Response Team (ICS- CERT) performed a research on the 2009-2013 period to see the trends in cyber attacks as regards the sectors that have been attacked.

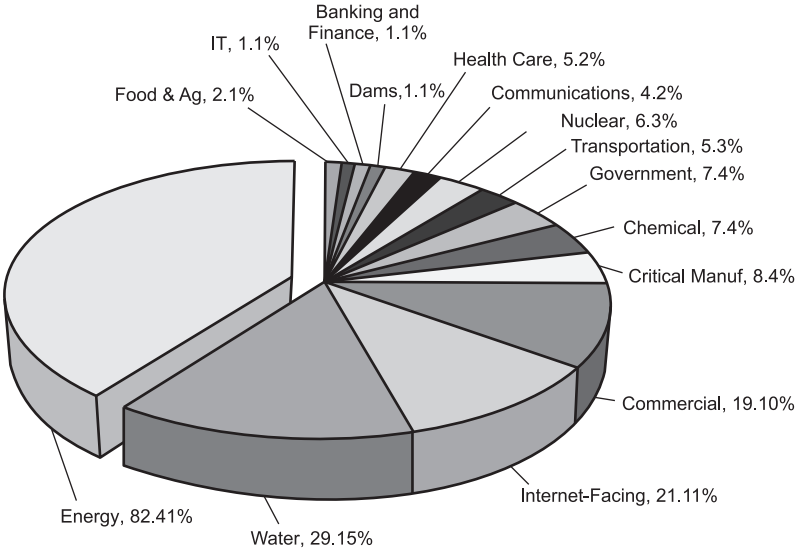
In 2009, the number of reported incidents was nine. The most attacked sectors were Water (3,34%) and Energy (3,33%)[3].

[3] ICS –CERT Incident Response Summary Report 2009-2011, available from: https://ics-cert.us-cert.gov/sites/default/files/documents/ICS-CERT%20Incident%20Response%20Summary%20Report%20(2009-2011)_accessible.pdf

In 2010 the number of reported incidents increased forty-one, with Energy as the leading sector with the 18, 44% of the total attacked. In 2010 the Nuclear sector was among those attacked with 5,12% due to the discovery of Stuxnet[4].

At the end of 2011 the reported incidents skyrocketed to 198, with 81,41% of them directed to the Water sector, followed by Energy, Nuclear, Government Facilities and Chemical[5].

Surprisingly, according to the ICS-CERT Operational Review of the fiscal year 2012 (October 2011–September 2012) the number of reported attacks is almost the same as in 2011, but with a complete change in the most attacked sector, that's to say energy, with 41% of the total reports[6].



Incident reports by sector (2012)

According to the ICS-CERT Operational Review of the first half of fiscal year 2013 (October 2012 — May 2013) the number of reported attacks is still increased with no change in the most attacked sector, that's to say energy, with 53%

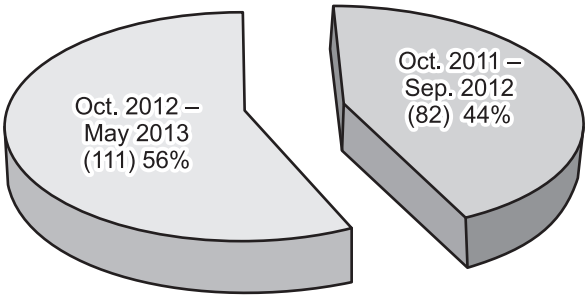
Given the fact that the above analyses encompasses only the incident reports of cyber attacks towards Critical Infrastructures that took place in the United States, it's not possible to draw any

[4] *Ibidem.*

[5] *Ibidem.*

[6] ICS-CERT Monthly Monitor Oct-Dec 2012, available from: http://ics-cert.us-cert.gov/pdf/ICS-CERT_Monthly_Monitor_Oct-Dec2012.pdf

general conclusion. However it's interesting to point out how the number of incidents related to cyber attacks, and also the sectors involved, increased substantially from 2010 onwards.



Energy is the most targeted sector

Common vulnerabilities and methods of attack

Vulnerabilities

the reason why the operators of cyber infrastructures — or infrastructures that rely on IT systems — should increase their focus on resilience is quickly explained if considering all of the "known" vulnerabilities and methods of attack that can negatively affect the lifecycle of cyber systems (and services depending on those systems).

The most recurring vulnerabilities and attacks can be briefly summarized in the following lists [3]:

Vulnerabilities

- Intrinsic software/hardware vulnerability (by design);
- Lack of (physical and logical) protection measures;
- 0-day vulnerabilities;
- Misconfiguration/incompatibility of the components of a system;
- Lack of software/hardware updates or updates not properly tested before installation/implementation;
- Unpreparedness of the system administrators;
- Lack of training of the users of the system;
- Obsolescence of the infrastructure or of part of the systems;
- Flaws in the corporate IT policy (credentials still active even after retiremet/resignement/dismissal of employees);

• Underestimation of risks deriving from physical vulnerabilities of facilities that hosts cyber systems (e.g. exposed to flooding, wilful acts, etc.).

Attacks

• Distributed denial-of-service;
• Network intrusions;
• Malware, trojan horse, backdoors;
• Targeting of specific users (administrators — key position's operator);
• Targeting of specific equipment/devices (e.g. Programmable logic controller — PLC);
• Total or partial destruction of the systems (e.g. fire, explosion, etc.);
• Social engineering;
• Insiders.

Both the aforementioned categories have increased in importance (and capability to harm cyber systems) due to the massive adoption of technologies in all of the corporate and public sectors and due to the light-speed evolution of the market competition — circumstance that in some case is forcing the technology vendors to sell "not-fully-tested" equipment.

It can be affirmed that the adoption of resilience measures seems to be justified by the same variables that a long time ago have suggested the adoption of protection measures and from the awareness that there's no resilience without protection and vice-versa.

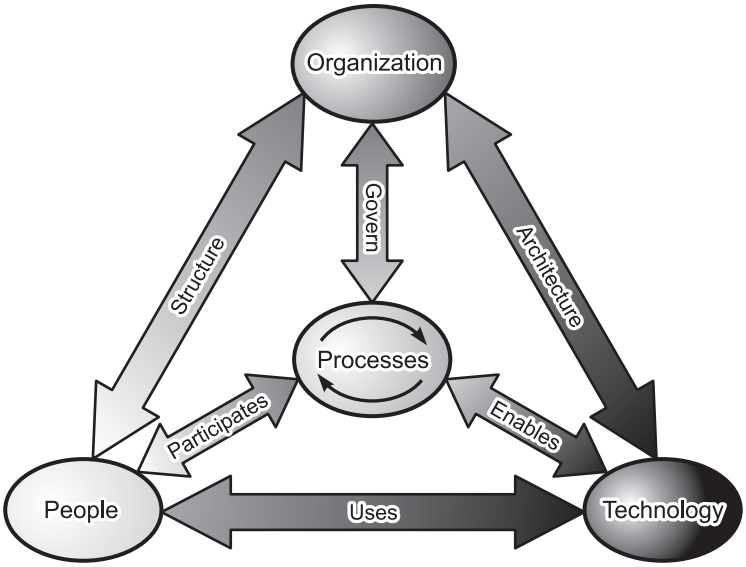
At the same time, it's necessary to highlight that the adoption of resilience measures shouldn't in any case divert or reduce the focus from protection, as these approaches are complementary and cannot be equally missing from the management and security lifecycle of modern infrastructures.

The resilience approach

past and recent experiences have shown how likely is that protection policies, sooner or later, may fail. For this reason, and being aware of the fact that the efforts put in place for protection of CIIs can be easily bypassed, all of the stakeholders involved in the security of such delicate and vital infrastructure are strongly suggested to put more emphasis on critical infrastructure resilience.

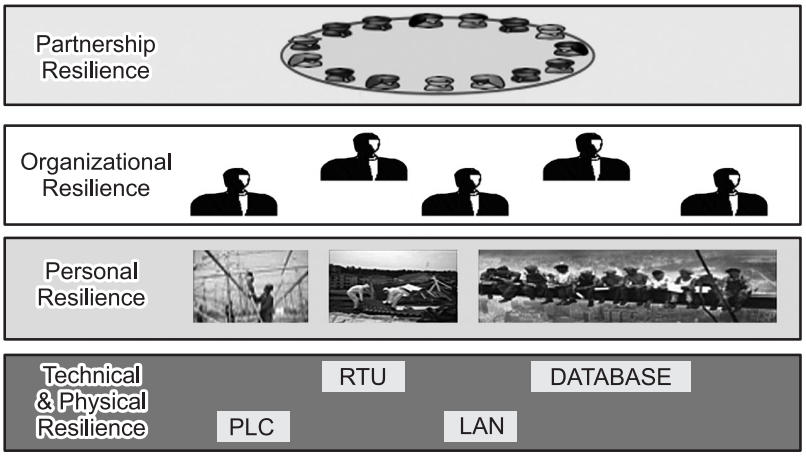
A Critical Infrastructure is not only made of technologies but especially of people, processes and organizations. The Risk Analysis

and Risk Management must take in consideration all these components, plus cultural background, to be complete and successful.



With the clear intention of proposing an embryonic approach for establishing a cyber resilience policy, it can be said that such policy should based on four lines of defence.

The first line of defence is at technical and physical level. Physical and technical resilience describe what the Critical Infrastructure has, in terms of implemented tangible safeguards to deter or slow down an adversary (fences, locks, bars, etc.), detect an attack (guards, sensors, electronic access control systems, etc.), and/or to mitigate vulnerabilities (shortcomings or weaknesses in the security posture). Traditional network security controls like firewall, intrusion prevention system, and anti-virus are widely deployed and adequate to keep known threats at bay, but are insufficient to mitigate the risk that is unknown (eg. 0-day vulnerabilities), unperceived (eg. lack of training or the presence of insiders) or that can be properly addressed (eg. software/hardware limits or the infrastructure's obsolescence). These legacy controls are often the key line in defense against these evolved threat actors, many of whom have access to sophisticated R&D resources. While the adversary innovates, in fact, the majority of security infrastructures continue to use dated technology as their primary defence [4].



Four lines of defense for modern resilience

The second line of defence is at personal level. Personal resilience is a critical component of systems' resilience. The personal resilience gap of greatest concern is not in defining employer-specific roles and responsibilities an employee has in an emergency. It lies in the employees' own personal preparedness so the employees are available more quickly and with better focus to the organization that relies on them to carry out their emergency roles and responsibilities when emergencies occur. Creating a company's culture of resilience it's already an urgent need that will require to change the way companies perceive themselves in relation to a disaster or an emergency. In an increasingly volatile and uncertain world, one of the greatest assets an organization can have is the agility to survive unexpected emergency situations [5].

The third line of defence is at organizational level. It is suggested that organizational resilience is best achieved through a systematic decomposition of its elements, based on discernible criteria. This breakdown isolates each of the components and facilitates the identification of key attributes or characteristics. The major pillars of organizational resilience are technical resilience and personal resilience, as described above, and functional resilience intended as a clear responsibility and definition of what to do and who does it [6].

A fourth line of defence is the establishment of collaboration and partnership among different stakeholders. In Europe, the European Public Private Partnership for Resilience (EP3R) was estab-

lished as a follow-up to the policy initiative on Critical Information Infrastructure Protection (CIIP) adopted by the European Commission on 30 March 2009. The objectives of EP3R are to support Information sharing and stock taking of good policy and industrial practices, and foster common understanding, discuss public policy priorities, objectives and measures, improve the coherence and coordination of policies for security and resilience in Europe and identify and promote the adoption of good baseline practices for security and resilience[7].

International approaches on resilience

On February 7th 2013, the "Cybersecurity Strategy of the European Union: an Open, Safe, and Secure Cyberspace"[8] was presented through a press conference with the important remarks of Catherine Ashton[9], EU high representative, Neelie Kroes[10], Vice-President of the European Commission responsible for the Digital Agenda and Cecilia Malmström[11], EU Commissioner for Home Affairs. The remarks revolve around the fact that we rely on cyberspace in almost every sector of our lives, and thus the importance of defending it from cyber attacks. Neelie Kroes underlines one of the critical point of the EU Strategy, that's to say cyber resilience: "We need to protect our networks and systems, and make them resilient. That can only happen when all actors play their part and take up their responsibilities. Cyber threats are not contained to national borders: nor should cyber security be. So our strategy is accompanied by a proposed Directive to strengthen

[7] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r

[8] European Commission (2013), *Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyberspace.,* available from: http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/join_2013_1_en.pdf

[9] Remarks by EU high representative Catherine Ashton at the at press conference on the launch of the EU's Cyber Security Strategy, February 7th 2013, available from: http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/EN/foraff/135287.pdf

[10] Neelie Kroes, "*Using cybersecurity to promote European values",* speech at the at press conference on the launch of the EU's Cyber Security Strategy, February 7th 2013, available from: http://europa.eu/rapid/press-release_SPEECH-13-104_en.htm

[11] Cecilia Malmström, "*Stepping up the fight against cybercriminals to secure a free and open Internet",* speech at the at press conference on the launch of the EU's Cyber Security Strategy, February 7th 2013, available from: http://europa.eu/rapid/press-release_SPEECH-13-105_en.htm

cyber-resilience within our single market. It will ensure companies take the measures needed for safe, stable networks. [...] Europe needs resilient systems and networks. Failing to act would impose significant costs: on consumers, on businesses, on society. A single cyber incident can cost from tens of thousands of euros for a small business — to millions for a large-scale data breach. Yet the majority of them could be prevented just by users taking simple and cheap measures."[12]

On 12th February 2013, the president of the United States Barack Obama issued an Executive Order entitled "Improving Critical Infrastructure Cyber security"[13], which has similar contents and measures to those included in the Cyber security strategy of the European Union.

On March 19th, 2013 the much awaited and coveted Cyber security Decree[14] (DPCM January 24th, 2013) was published in the Italian Official Gazzette. The Decree sets forth the new government architecture that is entrusted with the task of facing potential cyber security threats in Italy.

The Prime Minister is at the top of the organisational structure established by the Decree along with the "Committee for the Security of the Italian Republic" (CISR), which has the task of defining national security strategy (the so-called "National Cyber Security Strategy"). A "collegial co-ordination body" supports the first level of such organizational structure. The collegial co-ordination body is chaired by the Director General of the Department for Information Security (DIS). The Military Adviser assisting the Prime Minister also attends the meetings of the collegial co-ordination body.

On February 2014 the Italian Presidency of Council of Ministers has publically released the "National Strategic Framework for Cyberspace Security"[15] and the "National Plan for Cyberspace Protection and ICT Security"[16].

The National Cyber security Strategic Framework sets out the strategic guidelines that must be pursued through a joint effort and

---

[12] Neelie Kroes remarks, op. cit.

[13] Barack Obama, "Improving Critical Infrastructure Cybersecurity" Executive Order of February 12, 2013, available from: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[14] Available at: http://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2013-03-19&atto.codiceRedazionale=13A02504&elenco30giorni=true

[15] Available at: http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf

[16] Available at: http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-cyber-security-plan.pdf

a coordinated approach of all key stakeholders of the national cyber security architecture identified by the Prime Minister's Decree of the 24th January 2013, under the coordination and guidance of the Committee for the Security of the Republic.

Undoubtedly, this is a sign of how an important challenge the cyber security of Critical Infrastructures — and of their ICS — is becoming in different contexts.

References

[1] Sandro Bologna, Alessandro Fasani, Maurizio Martellini: Cyber Security Deterrence and IT Protection for Critical Infrastructures, SpringerBriefs in Computer Science 2013, pp 57-72

[2] Paul Theron, Sandro Bologna: Critical Information Infrastructure Protection and Resilience in the ICT Sector, Book, IGI Global, 2013.

[3] Sandro Bologna, Stefano Mele, Alessandro Lazari, "Improving Critical Infrastructure Protection and Resilience against Terrorism Cyber Threats", NATO Advanced Research Workshop Managing Terrorism Threats to Critical Infrastructure — Challenges for South Eastern Europe" Belgrade, Serbia, May, 2014.

[4] General Dynamics 2010, Defending against cyber attacks with session-level network security.

[5] Ann Coos, Ronald Bearse, 2013, Strengthening Resilience of the Nation's Most Important Asset: People, The CIP Report, December 2013.

[6] Wayne Boone, 2014, Functional Resilience: The "Business End" of Organizational Resilience, The CIP Report, January 2014.

А.Н.Курбацкий

Белорусский государственный университет

Личная информационная безопасность и правила поведения в виртуальном пространстве

Похоже, мир слишком увлекся глобализацией и быстрым построением гражданского общества с использованием новых информационно-коммуникационных технологий (ИКТ). Мы поступаем как неразумный авангард в боевых действиях, который, пытаясь максимально быстро достичь победы, забывает про тылы. Мы забываем про наши тылы — национальные государства, национальные особенности менталитета, культуры, образования. Но мы должны помнить, чем обычно заканчиваются такие неподготовленные наступления. Конечно гражданское общество нужно строить, но ИКТ лишь необходимые условия для этого и нельзя скорость развития ИКТ жестко увязывать со скоростью развития общества. В частности, мы быстро погружаемся в виртуальный мир, но совершенно оказались не готовы к такому погружению и не заботимся о личной информационной безопасности. Традиционно мы привыкли, что нужно обеспечивать информационную безопасность государства, информационную безопасность крупного, в первую очередь транснационального, бизнеса (корпораций, холдингов и т.д.), личная же информационная безопасность остается в тени.

Как в реальном мире, так и виртуальном должны действовать некоторые социальные регуляторы поведения. Попытки принять такие нормы предпринимаются по сути с самого зарождения Интернета. К сожалению, их эффективность пока не высока.

Хотя уже положительно то, что проблемы правил поведения стали очень активно обсуждаться. Есть ряд предложений по правилам поведения со стороны бизнеса (например, компания Microsoft), со стороны государств и групп государств (Россия, ШОС, НАТО (Таллиннский проект)), рабочей группы экспертов при генеральном секретаре ООН.

Многие эксперты, выступая против национальных рамок Интернета, предостерегают о потенциальной опасности введения правил и норм поведения в Интернете. Но если бы это была простая среда общения: а так в этой среде осуществля-

ется бизнес, образовательный процесс, услуги электронного правительства и т.д. Мы все чаще осуществляем в этой среде целый ряд государственных функций (функций регулирования), которые, как правило, носят и национальные рамки. С оценкой значения Интернета, и созданного на его основе виртуального пространства, для общества и личности государства, можно сказать, сильно опоздали, а бизнес, особенно транснациональный оказался на переднем крае, но,к сожалению, только с точки зрения получения прибыли.

Кто же должен активно формировать правила? В первую очередь, эксперты, как со стороны государства, так и общества, и бизнеса. Вспомним историю. Интернет создавался, формировался и развивался на начальной стадии в сравнительно узком научно-экспертном сообществе со своими достаточно устоявшимися нормами, правилами, которые по сути автоматически функционировали и в зарождающемся виртуальном пространстве. Базовая технологическая архитектура Интернета изначально основывалась на саморегулировании, не предполагающем особой иерархии управления и идентификации лиц, получающих и передающих информацию. Но затем быстрый рост аудитории Интернета привел к тому, что Интернет превратился в глобальную инфраструктуру трансграничного информационного обмена, появилось глобальное виртуальное пространство, но базовые технологические особенности принципиально не изменились, а лишь модифицировались для удобства использования миллионами пользователями (уже, конечно, не экспертами).

Если вспомнить, то и в традиционном обществе правила поведения формировались по сути в экспертной среде — будь то религиозная среда, университетская среда, среда городских ремесленников, объединенных в гильдии и т.д.

То, что годится для экспертного сообщества, обычно напрямую не подходит для всего общества.

Экспертная среда, редко бывает независимой (даже если мы говорим об экспертной среде весьма условно независимого гражданского общества), она в существенной степени зависит либо от государства, либо от бизнеса. Учитывая значительную трансграничность виртуального пространства, соответствующую экспертную среду целесообразно было бы формировать как международную среду, при авторитетных международных структурах (ООН), вовлекая в процесс экспертов от всех заинтересованный сторон. Можно полностью согласиться с формулировкой, разработанной Рабочей груп-

пой по управлению Интернетом при Генеральном секретаре ООН: «Управление Интернетом» означает «разработку и применение правительствами, частным сектором и гражданским обществом, при выполнении ими своей роли, общих принципов, норм, правил, процедур принятия решений и программ, регулирующих эволюцию и применение Интернета». Важно стремиться сделать так, чтобы мнение экспертного сообщества оказывало большое воздействие на формирование мнения, как правительственных структур, так и влиятельных бизнес-структур.

Пока мы обсуждаем нужны или не нужны правила в виртуальном пространстве — мы теряем время. В реальном мире государство в существенной степени брало на себя внедрение и поддержание правил. Молодое поколение остается в виртуальном мире практически без всяких правил, и, соответственно, не обеспечивается личная информационная безопасность. А время проходит очень быстро, молодость проходит быстро, и поколения быстро сменяются. К сожалению, многие изменения происходят настолько стремительно, что мы не успеваем их даже фиксировать, и живем в плену иллюзий. Например, в традиционном понимании сегодня массово нет даже студенческой группы. Часто в молодежной среде отношения в социальных сетях виртуального пространства гораздо более значимые (в существенной степени из-за виртуальной комфортности), чем в рамках той же студенческой группы. Вспоминая процесс формирования национальных (страновых) элит (и как следствие, экспертного сообщества), именно студенческие группы университетов были существенным механизмом этого процесса.

Понятно, что нормы и правила можно рассматривать в контексте информационной безопасности глобальной сети. Информационная безопасность становится уникальным средством по сути силового воздействия на неугодных граждан, групп граждан, общественные организации, неугодные бизнес-структуры. Но это же распространяется и на неугодные государства, группы государств. При этом, опять не имея четких правил и норм, высока степень анонимности такого воздействия.

Сейчас много говорят о социальной ответственности бизнеса. Конечно, было бы идеальным, если бы бизнес был более социально ответственен за свою ИКТ-продукцию, включая и развитие виртуального пространства. Но, к сожалению, слишком раскрученная (иногда заведомо искусственно) кон-

куренция в сфере ИКТ за прибыль не даст решения этой проблемы за приемлемый срок.

Новые ИКТ порождают новые глобальные инициативы в виде комплексных глобальных проектов, которые включают целый ряд интегрируемых ИКТ. Мы часто не можем гарантировать безопасность в рамках одной ИКТ, что уж говорить, если они еще интегрируются. И если на прогнозирование функциональности таких проектов затрачиваются большие ресурсы и средства, то безопасность исследуется по остаточному принципу.

Для примера можно вспомнить, например, об Интернете вещей. Еще в середине 2009 года корпорация Ericsson огласила прогноз, согласно которому к 2020 году около 50 млрд различных электронных устройств в мире будут взаимодействовать с Интернетом. Естественно, подавляющая часть из них будет взаимодействовать без вмешательства человека (в M2M — интерфейсе). То есть в существенной степени Интернет станет «Интернетом вещей». Интересна инициатива США — Национальная стратегия по глобальной безопасности цепи поставок, которая была принята в январе 2012 года. С технологической точки зрения можно сказать, что данная стратегия укладывается в Интернет вещей. Одной из основных целей в этой стратегии является интегрированная всемирная сеть транспортных, почтовых путей, средств и инфраструктуры, посредством которых товары перемещаются от точки производства до конечного потребителя. Технологически, это сочетание навигационных технологий, RFID, Интернета и т.п.

Конечно, с точки зрения функциональной полезности все эти тенденции более-менее понятны. А вот как решить проблемы обеспечения информационной безопасности, в частности личной информационной безопасности, совсем не ясно. Пока не понятно, как будет в таких масштабах обеспечиваться надежность работы приборов и устройств, связанных Интернетом. Что будет происходить с накапливаемым от приборов в Интернете огромным количеством информации. Ведь эта информация будет и прямо, и косвенно связываться с конкретными людьми. Опять проблема личной информационной безопасности. И здесь не только дело в очевидной возможности использования такой информации спецслужбами, как, например, заявил глава ЦРУ Дэвид Петреус — новые онлайн-устройства — это сокровищница данных для его ведомства. Такие глобальные инициативы, как Интернет вещей (а вместе с ним «умные дома», «умный транспорт», «умные

города») приведут к еще более массовому производству программного обеспечения. В этот процесс будут вовлечены новые миллионы программистов, как правило, с достаточно низким уровнем подготовки. Ясно, что для обеспечения безопасности таких глобальных инициатив для человека, общества нужен надежный безопасный программный продукт. А вот этого массово мы пока гарантировать не можем. Нет пока таких технологий и методологий, которые позволяют быстро, и главное для бизнеса — дешево, производить надежный и безопасный программный продукт. В мире работают гигантские конвейеры производства программного продукта без должного обеспечения его безопасности и надежности. Ошибки в программных средствах способны нанести ущерб, который значительно превысит эффект от их использования. Несколько утрируя, можно сказать, что безопасность и человека, и общества, и государства все больше зависит от программного продукта.

Достаточно очевидно, что сегодня в очень динамичное время, чтобы стать лидером бизнеса, приходится действовать вне правил, их нарушать — и мало вероятно, что бизнес будет активно внедрять правила и нормы в виртуальном пространстве. Мало придумать нормы — их еще надо внедрить — а это процесс достаточно длительный и дорогостоящий. И эти затраты могут уменьшить конкурентоспособность бизнеса, практически всегда ориентированного на получение максимальной прибыли.

В этом плане больше можно рассчитывать на государство, которое сохраняет национальные границы и «хоть какие-то правила поведения в реальном мире».

С правилами поведения в виртуальном пространстве тесно связана личная информационная безопасность. Быстрое развитие ИКТ и глобализация ускоряют прозрачность человека в виртуальном пространстве. Готовы ли мы к такой прозрачности? Практически нет, по сути нет, разумного обеспечения личной информационной безопасности. Изменения глобального масштаба могут произойти гораздо быстрее, чем кажется. Уже сейчас явно заметны тенденции, когда все больше и больше личной информации заносится в онлайн-профайлы. Личная жизнь перестает быть личной. Этому активно способствуют и ИКТ, и политика компаний, продвигающих ИКТ. Посмотрите, можем ли мы использовать планшет в полностью автономном режиме, как лет десять назад ноутбук. Нет гарантий, что планшет обеспечивает личную информаци-

онную безопасность. Его практически невозможно использовать длительное время вне сети — его стандартная операционная среда постоянно требует каких-либо изменений. Приложения, установленные на нем, также постоянно нуждаются в изменениях, в апгрейте и т.д. Если не изменишь — нет гарантий, что в один прекрасный момент приложение или операционная среда вообще не заблокируются. Все это заставляет хотя бы иногда подключаться к глобальной сети. А любое подключение — это возможность нарушения личной информационной безопасности. Людей нельзя «подставлять», не обеспечив их личной информационной безопасности. Как заявил Эрик Шмидт в интервью TheWallStreetJournal, по достижении совершеннолетия многие сегодняшние подростки будут вынуждены менять имена и фамилии, поскольку сегодняшняя молодежь описывает каждый свой шаг в социальных сетях, практически не осознавая последствий своих действий. Взрослое поколение (которое ответственно за развитие виртуального пространства) и подставляет этих подростков. В существенной степени это вопрос образования и воспитания, которые все больше уходят в виртуальное пространство. Поэтому и нужны правила и нормы поведения.

Хотя в мире сейчас быстро ломаются и традиционные нормы поведения. Нормы хоть как-то «цементируют» общество, иначе распадемся на индивидов, которые в итоге могут перестать быть и личностью. По сути, мы можем разрушить само понимание общества, если «переборщим» с индивидуализацией. Пока виртуальное пространство больше способствует индивидуализации, но не через раскрытие способностей, а наоборот. В Интернете мы в любой момент можем уйти от общения — в обычном обществе так не получается. В результате все ускоряющегося дробления на мало связные между собой сообщества нормы поведения тяжело распространять. Скорее всего, добровольных норм поведения сегодня не хватит. Требуется сочетание организационно-правовых, технико-технологических, социально-нравственных методов.

Еще один аспект личной информационной безопасности. Нам дали бесконтрольный доступ к огромному потоку информации, казалось бы, появляются и огромные потенциальные возможности развития. Но мы плохо учимся и учим, как с этой информацией работать, чему можно верить, чему нет. Раньше, когда информация попадала в СМИ, она хоть как-то проходила экспертизу (цензура тоже своего рода экспертиза). А сейчас — мы не знаем об истинных мотивах автора той

или иной информации, но в силу традиций часто ей верим. А как в таком случае доверять информации о здоровье, лечении и т.д. Только эксперты, и то в своей сфере, способны хоть как-то определить достоверность информации. Можно еще привести массовую неэффективность прямолинейного использования в образовании информационных материалов из Википедии.

Говоря о похожести норм поведения в обычной жизни и виртуальном пространстве, нужно не забывать, что в обычном общении анонимность занимает доли процента, а в виртуальном — может доходить до 90%. И пропадает серьезный фактор необходимости отвечать за свои поступки.

A.N.Kurbatskiy
Belarus State University

Personal information security and the rules of conduct in information space

It seems that the world got too much carried away by globalization and rapid development of civil society by means of new information and communication technologies (ICT). We act as a foolish vanguard in battle, the one that forgets about back areas while trying to achieve victory as quickly as possible. We tend to forget about our back areas — nation states, specifics of national mentality, culture and education. But we must remember how such unprepared offense usually ends up. Of course, civil society should be developed, but ICTs provide only the prerequisite environment and the rate of ICT development cannot be rigidly linked with the rate of society development. In particular, we are quickly immersing in a virtual world, but as it turned out, are not ready for such a dive and do not care about personal information security. Traditionally, we are accustomed to the need to ensure information security of the state, information security of big, especially transnational, business (corporations, holdings, etc.), whereas personal information security remains in the shadows.

In both real and virtual world there should be certain social regulators of behavior. In fact, attempts to adopt such rules have taken place since the inception of the Internet. Unfortunately for the time being they have not been very efficient.

And at the same time it is good that the issues of rules of conduct have become a subject of a very active discussion. There are a number of proposals on the rules of conduct set forward by business (for example, Microsoft), by states and groups of states (Russia, SCO, NATO (Tallinn draft)), by UN Secretary General Group of Governmental Experts.

Many experts, being in opposition to the national boundaries of the Internet, warn that it is potentially dangerous to adopt such rules of conduct for the Internet. It would be valid if the Internet was simply an environment for communication, however it is an environment for business, educational process, e-government services, etc. In this environment we increasingly frequently exercise a number of state functions (regulations), which also tend to be within national framework. It can be said that the states

were too late in assessing the importance of the Internet and the virtual space for society and individuals; while business, especially transnational, appeared at the forefront, but unfortunately, only in terms of profit.

Who should actively formulate the rules? First of all, experts on behalf of government, society, and business. Let's recall history. At an early stage the Internet was created, formed and developed by a relatively narrow scientific and expert community with its fairly well-established rules and regulations, which as a matter of fact also functioned automatically in the emerging cyberspace. Basic technological architecture of the Internet was originally based on self-regulation which did not imply special hierarchy of management and identification of individuals receiving and transmitting information. But then, due to rapid growth of the Internet user base, it had become a global infrastructure for cross-border information exchange; global virtual space emerged, but basic technological features had not been fundamentally changed, only modified for the ease of use by millions of users (who certainly are not experts).

If we recall, in a traditional society the rules of conduct were in fact also formed in the environment of experts — whether that be a religious or university environment, or the environment of urban artisans, united in a guild, etc.

That what is suitable for the expert community is usually not directly suitable for the whole society.

Expert community is rarely independent (even if we are talking about the expert community of a rather conditionally independent civil society), it substantially depends on either state or business. Taking into consideration that virtual space is largely transboundary, it would be appropriate to form the corresponding expert environment as international one, under the auspices of reputable international organizations (UN), including experts from all stakeholders. One can fully agree with the wording developed by the UN Secretary General Working Group on Internet Governance: "*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.*" It is important to strive that the opinion of expert community has a greater impact on opinion of both the governmental bodies, and influential business structures.

We are wasting our time discussing whether or not there should be rules in virtual space. In the real world the state to a large extent

took upon itself the implementation and maintenance of rules. The young generation resides in the virtual world almost without any rules, and accordingly, personal information security is not provided. And the time passes very quickly, youth is gone quickly and generations change quickly. Unfortunately, many changes are occurring so rapidly that we have no time to keep track of them, and we live enthralled by illusions. For example, today there exist no student groups in traditional sense (on a massive scale). Youth relations in social networks of virtual space are often much more important (to large extent due to virtual convenience) than relations within the same student group. If we recall the process of forming of national (country-specific) elite (and as a consequence, of expert community), student groups in universities have always been an essential mechanism of this process.

It is clear that rules and regulations can be viewed from the standpoint of information security of global network. Information security becomes a unique instrument of in essence forced action against citizens, groups of citizens, non-governmental organizations, undesirable business structures. But the same applies to unwanted states or groups of states. Once again without clear rules and regulations, there is a high degree of anonymity of such actions.

Nowadays there are a lot of discussions about corporate social responsibility. Of course, it would be ideal if business was more socially responsible for its ICT products, including the development of virtual space. But unfortunately too hyped up (sometimes certainly artificially) competition for profit in the ICT sector will not provide a solution to this problem within a reasonable timeframe.

New ICTs create new global initiatives in the form of complex global projects, which include a number of integrated ICTs. We often cannot guarantee the security of a standalone ICT, let alone if they are integrated. And while a lot of resources are spent on functionality prediction of such projects, security research is given whatever funds remain.

Let's recall, for example, the Internet of things. Back in mid-2009, Ericsson corporation announced a forecast that by 2020 some 50 billion different electronic devices in the world will have Internet connection. Naturally, the vast majority of them will work without human intervention (over M2M — interface). Essentially, the Internet will become the «Internet of things». In this regard, the US National Strategy for Global Supply Chain Security, adopted in January 2012, is also interesting. From a technological point of view we can say that this strategy fits into the Internet of Things.

One of the main goals of this strategy is development of an integrated worldwide network of transportation, postal routes, facilities and infrastructures which facilitate the delivery of goods from point of production to the end consumer. Technologically, it is a combination of navigation technologies, RFID, Internet, etc.

In terms of functional utility these trends are more or less clear. But it is not clear how to solve the issues of information security, in particular of personal information security. It is not clear how the reliability of Internet-connected instruments and devices would be provided on such a scale. What will happen with huge amount of information accumulated by these devices on the Internet? And this information will be directly or indirectly attributed to specific people. Again, it is the issue of personal information security. And the issue is not only about the obvious possibility that such information may be used by secret services, as David Petraeus, the head of the CIA, once said — the new online devices are a treasure trove of data for the Agency. Such global initiatives as the Internet of things (and with it — «smart home», «smart transportation», «smart city») will lead to more mass-produced software. This process will involve millions of new programmers with, as a rule, insufficient level of training. Clearly, to ensure the security of global initiatives for society and individuals we need secure and reliable software. But for time being these qualities cannot be guaranteed on a large scale. As of now there are no technologies and methods that would allow fast and, more importantly for business — inexpensive production of reliable and secure software. In the world there are giant conveyors for software production that do not provide proper safety and reliability. Errors in software can lead to damage, which greatly exceeds the effect of their use. If we exaggerate a little, we can say that the safety of individuals, society and the state becomes increasingly dependent on software.

It is quite obvious that today in such a dynamic time to become a business leader it is necessary to act outside the rules, break them — and it is unlikely that business will actively implement rules and regulations in virtual space. To formulate the norm is not enough — it has to be implemented — and this process is very time consuming and expensive. And these costs can reduce the competitiveness of business, the goal of which is almost always to maximize profits.

In this regard, it is better to look to the nation-states, as they retain national boundaries and «at least some rules of behavior in the real world».

Personal information security is closely associated with the rules of behavior in the virtual space. The rapid development of ICTs and globalization accelerate the transparency of individual in the virtual space. Are we ready for such transparency? Practically not, as in fact there exists no reasonable ensuring of personal information security. Changes on a global scale can happen a lot faster than one can think. Now we can see a clearly visible trend that more and more personal information is stored in online profiles. Personal life ceases to be personal. This trend is actively promoted by both ICTs and policies of ICT companies. See if we can use tablets completely offline, the same way we would use a laptop ten years ago. There is no guarantee that tablets provide personal information security. It is virtually impossible to use it offline for a long period of time — its standard operating system constantly requires adjustments. Installed applications also constantly require adjustments, updates etc. If you don't make these adjustments — there is no guarantee that at one point application or operating system will not lock up. All this entails you to be connected to the global network at least occasionally. And any connection means the possibility of personal information security violation. People should not be «crossed up» by not ensuring their personal information security. As Eric Schmidt said in an interview to The Wall Street Journal, upon reaching adulthood many of today's teens will have to change their names, because the young people of today describe each their step in social networks, almost unaware of the consequences of their actions. It is adult generation (which is responsible for the development of virtual space) that crosses these adolescents up. To great degree this is a question of education and training, and they increasingly retreat to virtual space. And therefore we need rules and norms of behavior.

Nowadays, however, traditional norms of behavior are being rapidly broken up as well. Norms somehow «bond» the society; otherwise it will fragment into individuals who may eventually cease to be personalities. In fact, we can destroy the very concept of society, if we go «too far» with individualization. For the time being virtual space greatly contributes to individualization — although not through development of abilities, but the other way around. On the Internet, we may at any time withdraw from communication — that does not happen in regular society. As a result of accelerated fragmentation into loosely connected communities, it is difficult to propagate norms of behavior. It is likely that today voluntary codes of conduct will be insufficient. We require a com-

bination of organizational, legal, technical, technological, social and moral practices.

Yet another aspect of personal information security. We have been given unsupervised access to a huge flow of information, and it brings, as it would seem, a huge potential for development. But we equally poorly study and teach how one should process this information, what should and what should not be believed. Previously, when the information was distributed by mass-media, it was somehow examined (censorship is also a kind of expertise). And now we do not know the real motives of the author of information, but due to traditions often believe it. And how in this case can we trust information about health or treatment, etc. Only experts with corresponding expertise are somehow able to determine the accuracy of the information. There are also examples of greatly inefficient straightforward use of information from Wikipedia in education.

Speaking about the similarity of ethics in everyday life and in virtual space, one must not forget that in the course of an ordinary communication there is a fraction of anonymity, while during virtual communication — it can reach up to 90%. And there is no factor of accountability for actions.

Кеир Гилс

Центр исследований конфликтов, Великобритания

Легитимизация онлайн-слежки и мониторинга

На момент написания этой статьи прошел почти год с тех пор, как мир впервые услышал имя Эдварда Сноудена. С того момента, когда он начал свою кампанию по распространению украденных секретных материалов о возможностях США и их союзников по ведению шпионажа, прошло некоторое время, и первоначальная реакция на это событие утихла. Соответственно, можно начинать делать выводы о долгосрочных последствиях его действий.

Помимо того, что национальной безопасности Соединенных Штатов и их стран-партнеров, а также борьбе с организованной преступностью и терроризмом во всем мире был нанесен серьезный ущерб, действия Сноудена и его сообщников вызвали и другие последствия, которые едва ли были запланированными. Они непреднамеренно ускорили развитие двух ранее существовавших направлений использования Интернета. В глобальном масштабе они ускорили изменение отношения пользователей Интернета к идеальному балансу между конфиденциальностью и безопасностью. А, в частности, в евроатлантическом сообществе, они ускорили движение к легитимизации мониторинга и слежки за деятельностью в Интернете. В настоящей статье рассмотрены оба направления развития и влияние, оказанное на них действиями Сноудена.

Отношение к правам и безопасности

Раскрытие Сноуденом в июне 2013 года информации о разведывательной деятельности США вызвало на международной арене ожесточенные споры по вопросу о законности и моральности мониторинга систем связи. Однако общественное обсуждение в США, Европе, и за ее пределами, выявило многообразие различных позиций по этим вопросам.

В последнее время рост доли не-англоязычной части пользователей Интернета привел к быстрому отходу от евроатлантических взглядов на природу Интернета, его регулирование, и регламентацию его свобод. В 1996 году более 66% пользователей Интернета находилось в США, в то время как в

2012 году на долю США приходилось лишь 12%[1]. По одной из оценок, на март 2012 года ежегодный рост числа пользователей Интернета в Индии составил 32%[2].

Одним из последствий этого сдвига является изменение усредненного мнения пользователей Интернета о наиболее подходящем балансе между конфиденциальностью и безопасностью в Интернете. В глобальном масштабе среднестатистический пользователь Интернета больше не разделяет взглядов «англосферы» к правам личности, которые, в сравнении с другими культурными традициями, там были традиционно значительно сильнее, чем государственные интересы. А именно, в настоящее время существенно изменилось усредненное отношение к легитимности деятельности по мониторингу и наблюдению за условно частными коммуникациями и действиями в Интернете, осуществляемой для противодействия терроризму и преступности, и для шпионажа.

Сложившуюся тенденцию необходимо разъяснить. Во всех обсуждениях поведения пользователей в Интернете отмечается, что очень небольшое число пользователей хоть как-то задумываются о конфиденциальности или проблеме безопасности. Большинство пользователей во всём мире продолжают совершать покупки и заходить в социальные сети, не беспокоясь о том, кто и для каких целей осуществляет наблюдение за ними. Кроме того, необходимо четко разделять усредненное отношение общества в целом и публичные заявления политических лидеров — с их «показным возмущением»[3]. Однако думающее меньшинство пользователей в вопросе соотношения конфиденциальности и безопасности государства или общества отходит от либеральных западных взглядов.

Как следствие, когда англоязычные СМИ, приняв на себя роль хранителей и арбитров, решили, в соответствии со своим собственным пониманием национальной безопасности[4], опубликовать секретную информацию, это не было отраже-

---

[1] "State of the Internet in Q3 2012", comScore, December 5, 2012, http://www.comscore.com/Insights/Presentations_and_Whitepapers/2012/State_of_the_Internet_in_Q3_2012

[2] "State of the Internet in Q1 2012", comScore, available at http://www.slideshare.net/alcancemg/state-of-theinternetq12012webinar-copy

[3] Bérénice Darnault, "Why the EU response to NSA leaks is contradictory", The World Outline, October 28, 2013, http://theworldoutline.com/2013/10/eus-response-nsa-leaks-spying-scandal-contradictory/

[4] "Guardian worldview at root of national security row", *The Commentator*, October 10, 2013, http://www.thecommentator.com/article/4250/guardian_worldview_at_root_of_national_security_row

нием отношения пользователей англоязычного Интернета, и тем более пользователей Интернета в мировом масштабе. Решения редакции и политика, например, британской газеты Guardian, отражали отношение некоторой части её либеральной аудитории — и нигде более такой гневной риторики не наблюдалось.

Легитимизация

Кроме рассмотренного изменения взглядов, заметна другая тенденция, особенно в международном сообществе Северной Атлантики и Западной Европы. Евроатлантическая область традиционно является оплотом прав и свобод личности, однако общественное обсуждение (которое стало возможным после того, как прошли первоначальный шок и возмущение, вызванные обвинениями Сноудена) также выявило явное движение в сторону принятия мониторинга и наблюдения в Интернете, вплоть до активной легитимизации.

Это движение принимает две четко выраженные формы: введение нового законодательства, охватывающего мониторинг и деятельность по наблюдению, и обеспечивающего для них прочную правовую основу; или подтверждение в ходе общественных обсуждений, что, в соответствии с действующим законодательством, эта деятельность уже является законной. Существуют примеры действий государств в обеих категориях, и они будут рассмотрены ниже, после изучения опыта Германии, который является подтверждающим правило исключением.

Внезапное и бесконтрольное раскрытие существования оказывающих воздействие на Германию систем мониторинга и надзора, вызвало интересные общественно-политические реакции, которые частично связаны с уникальной историей Германии в Европе, как нации, которая была разделена на государство с сильным уважением прав человека, и государство, где существовал всеобъемлющий государственный надзор и контроль населения.

Хотя в современной Германии конфиденциальность и защита данных рассматриваются как основные права, и их обеспечение является важным вопросом, первоначальная реакция на раскрытие деятельности Агентства национальной безопасности США (АНБ) по мониторингу Интернета была спокойной. В августе 2013 года глава канцелярии федерального канцлера и Федеральный министр по особым по-

ручениям Рональд Пофалла, заявил, что АНБ и Центр правительственной связи Великобритании (ЦПС) действовали в соответствии с немецким законодательством[5], и что скандал «окончен»[6].

Однако впоследствии, в октябре 2013 года, стало известно, что под наблюдением американских агентств был личный мобильный телефон канцлера Ангелы Меркель[7]. В ходе расследования, которое в Германии стало известно как «Handygate», были выявлены новые факты слежки за гражданами и лидерами Германии. Общественное осуждение подкреплялось утверждениями, что наблюдение за бундестагом осуществлялось из находящегося по соседству американского посольства. Сильная негативная реакция против мониторинга и наблюдения была вызвана и тем, что посольство находится под особой защитой немецких полицейских и военных, и было высказано предположение, что деньги немецких налогоплательщиков были использованы для защиты системы наблюдения за немецкими лидерами и гражданами[8].

Первоначальные заверения правительства о законности всех действий, отказ поддержать общественные интересы, и последующее внезапное и шокирующее раскрытие информации комментаторы сравнивали с возведением Берлинской стены в 1961 году. Германия была вынуждена выразить своим американским союзникам публичный протест и объявить о возможных потенциальных серьезных последствиях для будущих законных операций наблюдения в Германии[9]. Это произошло ввиду общественных опасений, направленных в первую очередь на США, и заявлений, что «США являются

---

[5] Carstens, Peter, "Pofalla: Amerikaner und Briten halten sich an deutsches Recht", Frankfurter Allgemeine Zeitung, August 1, 2013, http://www.faz.net/aktuell/politik/inland/spaehaffaere-pofalla-amerikaner-und-briten-halten-sich-an-deutsches-recht-12528037.html

[6] "Pofalla erklärt NSA-Affäre für beendet", Die Zeit, August 12, 2013, http://www.zeit.de/politik/deutschland/2013-08/nsa-bnd-pofalla--bundestag-spaehaffaere-snowden-abkommen

[7] "Zu Informationen, dass das Mobiltelefon der Bundeskanzlerin möglicherweise durch amerikanische Dienste überwacht wird", Bundesregierung Pressemitteilung, October 23, 2013, http://www.bundesregierung.de/Content/DE/Pressemitteilungen/BPA/2013/10/2013-10-23-merkel-handyueberwachung.html

[8] Smale, Alison, "Anger Growing Among Allies on U.S. Spying", The New York Times. October 23, 2013, http://www.nytimes.com/2013/10/24/world/europe/united-states-disputes-reports-of-wiretapping-in-Europe.html?_r=0

[9] Troianovski, Anton, "Germany Warns of Repercussions from U.S. Spying", The Wall Street Journal, October 28, 2013, http://online.wsj.com/news/articles/SB10001424052702304200804579163760331107226

не единственной страной, которая, по мнению немецкой разведки, может шпионить за руководством страны»[10].

Однако в других странах история и социально-культурные особенности вызвали совершенно иную реакцию. США и Великобритания являются примерами стран, где было подтверждено, что мониторинг и слежка являются законными, в соответствии с действующим законодательством.

Взгляды США и Великобритании

В США продолжается непростое обсуждение но, как представляется, оно подходит к выводу, что сами мероприятия были законными, но система, обеспечивающая надзор над ними, не подходила для этой задачи и требовала корректировки и большей прозрачности[11].

На общественное обсуждение в Великобритании оказала влияние её особая роль в двух ключевых аспектах, связанных с раскрытием фактов Интернет-слежки. Это, во-первых, важная роль ЦПС, как партнера АНБ по осуществлению наблюдения. Во-вторых, важная роль газеты «the Guardian» в распространении украденной секретной информации о предполагаемой деятельности по слежке.

Выступление начальников трех британских разведывательных служб и служб безопасности в парламентском Комитете по вопросам разведки и безопасности[12], которое произошло после первоначального смятения и беспокойства по поводу сенсационных новостей о заявлениях Сноудена, оказало значительное влияние на общественное мнение[13]. После этого появились признаки, что даже самые либерально настроенные наблюдатели начинали осознавать уровень ущерба, причиненного безрассудным крестовым походом газеты «the

---

[10] Anton Troianovski, "Germany to Boost Anti-Spy Efforts", *Wall Street Journal*, November 20, 2013, http://online.wsj.com/news/articles/SB10001424052702304791704579209740311164308

[11] По материалам "Power and Commerce in the Internet Age", Chatham House, London, November 25-26 2013, available at http://www.chathamhouse.org/Internet2013/agenda

[12] Intelligence and Security Committee open evidence session, November 7, 2013, UK Parliament website, http://www.parliamentlive.tv/Main/Player.aspx?meetingId=14146

[13] Catherine A. Traywick, "British Spies Aren't James Bonds, and 7 Other Things We Learned from Britain's Landmark Intelligence Hearing", *Foreign Policy*, November 7, 2013, http://blog.foreignpolicy.com/posts/2013/11/07/british_spies_arent_james_bonds_and_7_other_things_we_learned_from_the_uks_landmar

Guardian»[14]. Результат проявился в общественном мнении по вопросу Интернет-слежки в Великобритании. Опрос показывает, что «более 60%» респондентов считают, что спецслужбы имеют столько возможностей для мониторинга активности в Интернете, сколько нужно, или что им необходимо больше возможностей. И это несмотря на то, что есть понимание необходимости большей прозрачности и «осознанного диалога с общественностью»[15]. Представляется, что в целом общественное мнение в Великобритании соответствует взглядам, отраженным в американских опросах — раскрытие секретной информации об Интернет-слежке нанесло ущерб национальной безопасности[16] — к явному разочарованию либерально настроенных журналистов в том, что остальная часть Великобритании не придерживается их точки зрения[17]. Было высказано мнение, что в Великобритании это результат более четкого осознания находящихся под угрозой интересов безопасности. Как описано в Financial Times:

«Основная часть истории Великобритании... это повествование о стране, которой приходилось противостоять последовательным попыткам иностранных вторжений. Роль спецслужб в защите Великобритании высоко отмечена и прославляется... Большинство британских граждан принимают и, более того, ценят роль государственной власти в обеспечении свободы и независимости страны — а деятельность спецслужб исторически была неотъемлемой частью этих задач. Теракты в Лондоне в 2005 году свидетельствуют о том, что угроза терроризма только усилила осознание потребности в хороших разведслужбах»[18].

---

[14] Andrew Sparrow, "Guardian faces fresh criticism over Edward Snowden revelations", *The Guardian*, November 10, 2013, http://www.theguardian.com/media/2013/nov/10/guardian-nsa-revelations-edward-snowden

[15] UK Home Secretary Hazel Blears, speaking at Intelligence and Security Committee open evidence session, November 7, 2013, UK Parliament website, http://www.parliamentlive.tv/Main/Player.aspx?meetingId=14146

[16] Scott Clement, "Poll: Most Americans say Snowden leaks harmed national security", *The Washington Post*, November 20, 2013, http://www.washingtonpost.com/politics/poll-most-americans-say-snowden-leaks-harmed-national-security/2013/11/20/13cc20b8-5229-11e3-9e2c-e1d01116fd98_story.html

[17] John Naughton, "Edward Snowden: public indifference is the real enemy in the NSA affair", *The Observer*, October 20, 2013, http://www.theguardian.com/world/2013/oct/20/public-indifference-nsa-snowden-affair

[18] Gideon Rachman, "Why the British like their spies", *Financial Times*, November 10, 2013.

Взгляды в Европе

В отличие от Великобритании, в ряде европейских стран движение к публичной легитимизации Интернет-слежки и надзорной деятельности приняло форму нового законодательства. Многие европейские страны сделали шаги по созданию или укреплению прочной юридической основы для своей деятельности по перехвату и наблюдению.

Неожиданной была реакция Северных стран-членов ЕС на связанные со Сноуденом события. Ввиду специфического восприятия угроз и ясного осознания уязвимости, общественные обсуждения в странах Северной Европы (которые, как правило, являются убежденными сторонниками права на неприкосновенность личной жизни) не были такими жесткими[19]. В Финляндии новость о высокотехнологичной атаке и утечке данных из Министерства иностранных дел (ответственность за которую неофициальные источники возложили на Россию[20]) дала импульс общественному обсуждению возможных новых законов о легальном перехвате данных. При этом, большая часть обсуждений затрагивала не вопрос необходимости таких действий, а какому государственному органу лучше поручить их осуществление[21]. Несмотря на то, что в Швеции, в соответствии с законом «FRA», перехват уже легален, власти в настоящее время стремятся расширить свои полномочия[22]. Министр иностранных дел Швеции Карл Бильдт сказал, что сотрудничество с зарубежными спецслужбами по разведывательной деятельности против России «едва ли является сенсацией»[23]. А власти Дании были настолько уверены в законности своей деятельности, что раскрыли общую информацию о ранее засекреченных программах сбора данных для того, чтобы упредить распространение неверной

---

[19] "Swedes 'not afraid' of internet surveillance", *The Local*, November 8, 2013, http://www.thelocal.se/20131108/swedes-not-worried-about-internet-surveillance-survey

[20] Keir Giles, "Cyber Attack on Finland is a Warning for the EU", Chatham House, November 8, 2013, http://www.chathamhouse.org/media/comment/view/195392

[21] "Verkkovalvonta keskittymässä yhdelle taholle", *Ilta-Sanomat*, 18 November 2013, http://m.iltasanomat.fi/kotimaa/art-1288622010437.html

[22] "Intel agency seeks direct access to Swedes' data", *The Local*, November 19, 2013, http://www.thelocal.se/20131119/swedens-security-service-seeks-direct-data-access

[23] "Bildt defends Sweden surveillance", *The Local*, November 3, 2013, http://www.thelocal.se/20131103/bildt-defends-sweden-surveillance

информации журналистами, которые получили материалы Сноудена[24].

В других странах Европы есть много разных оценок законности перехвата сообщений, даже в таких узких рамках вопроса конфиденциальности, как права человека. Согласно проекту «Руководства ЕС по правам человека по вопросам свободы слова онлайн и офлайн»,

«неуважение права конфиденциальности и защиты данных представляет собой ограничение свободы выражения мнений. Незаконное наблюдение за связью, перехват сообщений, а также незаконный сбор персональных данных нарушают право на неприкосновенность частной жизни и свободу выражения мнений»[25].

Однако в 2007 году Европейский суд по правам человека постановил, что жалоба итальянского Интернет-пользователя, которая основывалась на восьмой статье Европейской конвенции по правам человека (право на уважение частной и семейной жизни), не может быть рассмотрена (так как является явно необоснованной). Хотя жалоба касалась спама, а не наблюдения, суд постановил, что «получив доступ к Интернету, пользователи электронной почты больше не пользуются эффективной защитой своей сферы личной жизни»[26].

Теперь Италия, и, в особенности, Франция предпринимают меры по созданию национальной, а не европейской правовой базы для мониторинга и наблюдения. На момент написания совсем недавно, в декабре 2013 года, во Франции был принят закон, который позволяет вести наблюдение за Интернет-пользователями в режиме реального времени и без получения предварительных санкций. При этом оно может осуществляться гораздо более широким кругом представителей власти, в том числе полицией, жандармерией, разведслужбами и антитеррористическими ведомствами, а также несколькими министерствами[27]. Последовали обвинения в

---

[24] Claus Blok Thomsen, Jakob Sorgenfri Kjær, Jacob Svendsen, "Presset FE fortæller om dansk spionage", *Politiken*, November 20, 2013, http://politiken.dk/indland/ECE2138411/presset-fe-fortaeller-om-dansk-spionage/

[25] Draft "EU Human Rights Guidelines on Freedom of Expression Online and Offline", unpublished, version as at November 20, 2013.

[26] Muscio v. Italy, European Court of Human Rights, "Information Note on the Court's case-law No. 102", November 2007, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=002-2419

[27] "Adoption de la loi controversée de programmation militaire", *Le Monde*, December 10, 2013, http://www.lemonde.fr/international/article/2013/12/10/adoption-definitive-de-la-controverse-loi-de-programmation-militaire_3528927_3210.html

цинизме, так как этот закон был принят всего лишь через несколько недель после того, как официальный Париж выразил возмущение, что АНБ якобы осуществляло такую же деятельность, а президент Франсуа Олланд резко осудил её[28].

Таким образом, раскрытие информации о мероприятиях по слежке, осуществляемых, как предполагается, АНБ и ЦПС, ведёт к тому, что всё больше государств-партнеров США и Великобритании работают над созданием такой нормативно-правовой базы, которая даст им возможность участвовать в этой деятельности на неоспоримой законной основе. Раскрытие предполагаемых возможностей и охвата системы слежки США (и систем их союзников) привело к появлению в части англоязычных СМИ резких и возмущенных репортажей. Несмотря на это, общественное мнение пошло по иному пути. Напротив, более сбалансированная и трезвая оценка потребностей национальной безопасности ведёт ведущие государства Европы к принятию через демократические процедуры законов, направленных на обеспечение бесперебойного продолжения наблюдения в Интернете за отдельными угрозами безопасности.

Следовательно, несмотря на обеспокоенность проблемой конфиденциальности, предпринимаемые в Интернете активные меры предотвращения и упреждения угроз национальной безопасности будут по-прежнему восприниматься как легитимные. Можно ожидать, что новые условия повышенной информированности общественности не будут препятствовать этой деятельности. Эдвард Сноуден и его сообщники едва ли рассматривали эти результаты среди желаемых вероятных последствий своих обвинений в адрес АНБ.

---

[28] Kim Willsher, "French officials can monitor internet users in real time under new law", *The Guardian*, December 11, 2013, http://www.theguardian.com/world/2013/dec/11/french-officials-internet-users-real-time-law

Keir Giles
Conflict Studies Research Centre, UK

Legitimation of Online Surveillance and Monitoring

At the time of writing, it is almost one year since the world first heard the name of Edward Snowden. With the time that has passed since he began his campaign of distributing stolen classified records on US and allied espionage capabilities, some of the initial drama of the event has now faded and it is possible to begin to draw conclusions about the longer-term impacts of his actions.

Leaving aside the severe detriment to the national security of the United States and its partner nations, and to the fight against organized crime and terrorism globally, Snowden and his accomplices have caused other effects which were unlikely to have been intentional. They have inadvertently accelerated two previously existing trends in internet use: worldwide, a shift in the median attitude of internet users to the ideal balance between privacy and security; and in the Euro-Atlantic community specifically, a trend toward legitimation of monitoring and surveillance of online activities. This short paper will describe each of trends, and the effects on them of the Snowden defection, in turn.

Attitudes to Rights and Security

Disclosures of alleged U.S. surveillance activities to the public by Snowden in June 2013 sparked heated international debate on the legality and morality of telecommunications monitoring. But public discussion in the U.S., Europe, and beyond, revealed widely varying societal attitudes to the issues involved.

The recent growth of non-Anglophone online populations has led to a rapid movement away from Euro-Atlantic views of the nature of the internet and how it and its freedoms should be regulated. In 1996, the U.S. made up over 66% of the world's online population, whereas in 2012, it accounted for only 12%.[1] According to one assessment, India saw an increase in numbers of internet users of 32% just in the year to March 2012.[2]

[1] "State of the Internet in Q3 2012", comScore, December 5, 2012, http://www.comscore.com/Insights/Presentations_and_Whitepapers/2012/State_of_the_Internet_in_Q3_2012

[2] "State of the Internet in Q1 2012", comScore, available at http://www.slideshare.net/alcancemg/state-of-theinternetq12012webinar-copy

One effect of this shift is an adjustment in median attitudes of internet users to the ideal balance of privacy against security on the internet. The average global internet user no longer shares the Anglosphere's attitude to individual rights, which have traditionally been significantly stronger by comparison to those of the state than in other cultural traditions. Specifically, the average attitude to the legitimacy of monitoring and surveillance of notionally private communications and activities online, for the purpose of prevention of terrorism and crime and for espionage, is now also distinctly different.

This trend needs to be caveated: as with all discussion of user attitudes online, it is only a very small percentage of overall users that devote any thought at all to privacy or security issues. The majority of users worldwide continue to engage in their shopping and social media use without losing sleep over who is monitoring them or for what purpose. In addition, a clear distinction needs to be drawn between average societal attitudes overall, and the public statements of leadership figures, with their occasional "theatrical outraged reactions"[3]. But within that thinking minority of users, the importance accorded to individual privacy versus the security of the state or society is shifting away from liberal Western attitudes.

The consequence is that when sections of the English-language media appointed themselves to the role of gatekeepers and arbiters, deciding for themselves what classified information they would release to the public according to their own definitions of national security[4], this approach failed to reflect the overall attitudes of internet users in the Anglosphere, and even less so those of internet users overall. The editorial decisions and policy of, for example, the UK's Guardian newspaper, chimed with the attitudes of a percentage of its liberal readership — but the tone of outrage was not mirrored elsewhere.

Legitimation

Alongside this shift in attitude, another trend is discernable specifically in the North Atlantic and Western European international community. This Euro-Atlantic area has traditionally been a bastion of individual rights and freedoms: but the national debates

[3] Bérénice Darnault, "Why the EU response to NSA leaks is contradictory", The World Outline, October 28, 2013, http://theworldoutline.com/2013/10/eus-response-nsa-leaks-spying-scandal-contradictory/

[4] "Guardian worldview at root of national security row", *The Commentator*, October 10, 2013, http://www.thecommentator.com/article/4250/guardian_worldview_at_root_of_national_security_row

that became possible once the often false shock and outrage at Snowden's allegations had died down also showed a distinct movement towards acceptance, up to and including active legitimation, of online monitoring and surveillance.

This movement takes two distinct forms: either new legislation to cover monitoring and surveillance activity, and ensure that it is carried out on a sound legal basis, or confirmation through public debate that the activities are indeed already legitimate under existing legislation. National examples are available in both categories, and will be discussed below, after examining an exception that proves the rule: the case of Germany.

Sudden and uncontrolled disclosure of monitoring and surveillance systems affecting Germany triggered interesting socio-political reactions, partly related to Germany's unique history in Europe as a nation previously divided into one state with a strong respect for individual rights, and another where state surveillance and control of the population were all-pervasive.

Although privacy and data protection are major concerns in modern Germany and treated as fundamental rights, the initial German reactions to disclosures of NSA internet monitoring activities were untroubled. In August 2013, Ronald Pofalla, Chief of Staff of the German Chancellery and Federal Minister for Special Affairs, stated that the NSA and GCHQ had acted in accordance with German law[5], and that any scandal was now "over"[6].

Subsequently, however, it was reported in October 2013 that Chancellor Angela Merkel's personal mobile phone was under surveillance by U.S. agencies[7]. During investigation of what became known in Germany as the "Handygate affair", further monitoring of German citizens and leaders was revealed. Public disapprobation was fuelled by disconcerting allegations that the German Bundestag was being monitored from the nearby U.S. embassy. With the embassy under special protection by German police and

---

[5] Carstens, Peter, "Pofalla: Amerikaner und Briten halten sich an deutsches Recht", Frankfurter Allgemeine Zeitung, August 1, 2013, http://www.faz.net/aktuell/politik/inland/spaehaffaere-pofalla-amerikaner-und-briten-halten-sich-an-deutsches-recht-12528037.html

[6] "Pofalla erklärt NSA-Affäre für beendet", Die Zeit, August 12, 2013, http://www.zeit.de/politik/deutschland/2013-08/nsa-bnd-pofalla--bundestag-spaehaffaere-snowden-abkommen

[7] "Zu Informationen, dass das Mobiltelefon der Bundeskanzlerin möglicherweise durch amerikanische Dienste überwacht wird", Bundesregierung Pressemitteilung, October 23, 2013, http://www.bundesregierung.de/Content/DE/Pressemitteilungen/BPA/2013/10/2013-10-23-merkel-handyueberwachung.html

military services, the suggestion that German taxes had been used to protect an installation spying on German leaders and citizens contributed to a strong public backlash against monitoring and surveillance activities[8].

Commentators compared early bland government assurances that all actions were legal, and a refusal to engage with public concerns, followed by sudden and shocking disclosures, to the erection of the Berlin Wall in 1961. With public concern directed primarily at the United States, and only occasional reminders that "the U.S. isn't the only country German intelligence believes may be spying on the country's leadership"[9], Germany was forced to remonstrate publicly with its U.S. allies, with further potential severe implications for future legitimate monitoring operations within Germany[10].

Elsewhere, however, a different history and socio-cultural framework has led to entirely different reactions. The USA and UK are examples of nations where monitoring and surveillance has been confirmed as legitimate under existing legislation.

US and UK Attitudes

In the USA, the debate is complex and ongoing, but appears to be reaching the conclusion that the activities themselves were legal, but the system for ensuring their oversight was not fit for purpose and required adjustment and greater transparency[11].

The British debate is coloured by the particular role of the UK in two key aspects of the 2013 disclosures on internet surveillance: the prominent role of GCHQ as a partner of the NSA in facilitating surveillance, and the prominent role of The Guardian newspaper in disseminating stolen classified information on alleged surveillance activities.

After initial confusion and concern over sensationalised reporting of Snowden's allegations, the appearance before Parliament's

---

[8] Smale, Alison, "Anger Growing Among Allies on U.S. Spying", The New York Times. October 23, 2013, http://www.nytimes.com/2013/10/24/world/europe/united-states-disputes-reports-of-wiretapping-in-Europe.html?_r=0

[9] Anton Troianovski, "Germany to Boost Anti-Spy Efforts", *Wall Street Journal*, November 20, 2013, http://online.wsj.com/news/articles/SB10001424052702304708045791637603311072260479170457920974031116430 8

[10] Troianovski, Anton, "Germany Warns of Repercussions from U.S. Spying", The Wall Street Journal, October 28, 2013, http://online.wsj.com/news/articles/SB10001424052702304200804579163760331107226

[11] As outlined at "Power and Commerce in the Internet Age", Chatham House, London, November 25-26 2013, agenda available at http://www.chathamhouse.org/Internet2013/agenda

Intelligence and Security Committee of the chiefs of the three UK intelligence and security services[1] began a significant shift in public opinion[2]. Afterwards, there were indications that even the most liberal-minded of observers were beginning to realise the extent of the damage done by The Guardian's misguided crusade[3]. Public perception of internet surveillance in the UK shows the result. Polling suggests that "60% plus" say the intelligence services have the right amount of power to monitor activity on the internet or need more — even though there is a perceived need for more transparency and an "informed dialogue with the public"[4]. Broadly, UK public opinion appears to be in line with the perception reflected in U.S. polls that releasing classified information on internet surveillance was harmful to national security[5] — to the palpable frustration of liberal journalists that the rest of the UK does not see it their way[6]. It has been argued that this results from a higher British perception of the security interests that are at stake. As described in the Financial Times:

"*The basic narrative of British history... is of a country that has had to ward off a succession of attempted foreign invasions. The role of the intelligence services in protecting the UK is both noted and celebrated... Most British citizens accept and, indeed, celebrate the role of the state in keeping the country free and independent — and the role of the intelligence services has historically been integral to that task. The threat from terrorism, as witnessed in the London bomb-*

---

[12] Intelligence and Security Committee open evidence session, November 7, 2013, UK Parliament website, http://www.parliamentlive.tv/Main/Player.aspx?meetingId=14146

[13] Catherine A. Traywick, "British Spies Aren't James Bonds, and 7 Other Things We Learned from Britain's Landmark Intelligence Hearing", *Foreign Policy*, November 7, 2013, http://blog.foreignpolicy.com/posts/2013/11/07/british_spies_arent_james_bonds_and_7_other_things_we_learned_from_the_uks_landmar

[14] Andrew Sparrow, "Guardian faces fresh criticism over Edward Snowden revelations", *The Guardian*, November 10, 2013, http://www.theguardian.com/media/2013/nov/10/guardian-nsa-revelations-edward-snowden

[15] UK Home Secretary Hazel Blears, speaking at Intelligence and Security Committee open evidence session, November 7, 2013, UK Parliament website, http://www.parliamentlive.tv/Main/Player.aspx?meetingId=14146

[16] Scott Clement, "Poll: Most Americans say Snowden leaks harmed national security", *The Washington Post*, November 20, 2013, http://www.washingtonpost.com/politics/poll-most-americans-say-snowden-leaks-harmed-national-security/2013/11/20/13cc20b8-5229-11e3-9e2c-e1d01116fd98_story.html

[17] John Naughton, "Edward Snowden: public indifference is the real enemy in the NSA affair", *The Observer*, October 20, 2013, http://www.theguardian.com/world/2013/oct/20/public-indifference-nsa-snowden-affair

ings of 2005, has only increased the awareness of the need for good intelligence"[18].

Attitudes in Europe

Unlike in the United Kingdom, in several European nations the move towards public legitimation of internet interception and surveillance activities has taken the form of new legislation. A number of European countries have moved to establish or reinforce a firm legal framework for their own interception and surveillance activities.

Nordic EU member states have challenged assumptions with their reactions in the aftermath of the Snowden defection. The debate in Nordic countries, which might ordinarily have been expected to be staunch advocates of privacy rights, has been tempered by a more specific threat perception and an acute awareness of the vulnerabilities of those states[19]. In Finland, news of a sophisticated attack and data breach at the Ministry for Foreign Affairs (MFA), which private sources blamed on Russia[20], gave impetus to public discussion of possible new laws on legal intercept — with much of the debate focusing not on whether this should take place, but under which government agency it would best fit[21]. In Sweden, although interception is already legal under the "FRA Law", the authorities are now seeking to enhance their powers[22]. Swedish Foreign Minister Carl Bildt described cooperation with foreign intelligence services on communications intelligence gathering against Russia as "hardly sensational"[23]. And authorities in Denmark felt sufficiently secure in the legitimacy of their work to pre-empt inaccurate reporting by journalists supplied

---

[18] Gideon Rachman, "Why the British like their spies", *Financial Times*, November 10, 2013.

[19] "Swedes 'not afraid' of internet surveillance", *The Local*, November 8, 2013, http://www.thelocal.se/20131108/swedes-not-worried-about-internet-surveillance-survey

[20] Keir Giles, "Cyber Attack on Finland is a Warning for the EU", Chatham House, November 8, 2013, http://www.chathamhouse.org/media/comment/view/195392

[21] "Verkkovalvonta keskittymässä yhdelle taholle", *Ilta-Sanomat*, 18 November 2013, http://m.iltasanomat.fi/kotimaa/art-1288622010437.html

[22] "Intel agency seeks direct access to Swedes' data", *The Local*, November 19, 2013, http://www.thelocal.se/20131119/swedens-security-service-seeks-direct-data-access

[23] "Bildt defends Sweden surveillance", *The Local*, November 3, 2013, http://www.thelocal.se/20131103/bildt-defends-sweden-surveillance

with Snowden material by going on the record to describe previously classified collection programmes[24].

Elsewhere in Europe, there are numerous and varying assessments of the legality of interception of communications, even within the narrow focus of privacy as a human rights issue. According to a draft of the "EU Human Rights Guidelines on Freedom of Expression Online and Offline",

"*lack of respect for the right of privacy and data protection constitutes a restriction of freedom of expression. Illegal surveillance of communications, their interception, as well as the illegal collection of personal data violates the right to privacy and freedom of expression*"[25].

Yet in 2007, the European Court of Human Rights ruled as inadmissible (manifestly ill-founded) a complaint by an Italian internet user under Article 8 (right to respect for private and family life) of the European Convention on Human Rights. Although the complaint related to spam rather than surveillance, the Court declared that "once connected to the Internet, e-mail users no longer enjoyed effective protection of their privacy"[26].

Now, Italy and especially France are moving to ensure that a national, rather than European, legal basis for monitoring and surveillance is in place. Most recently at the time of writing, a law was passed in France in December 2013 allowing surveillance of internet users in real time and without prior legal authorisation, by a much increased range of public officials including police, gendarmes, intelligence and anti-terrorist agencies as well as several government ministries[27]. The law gave rise to accusations of cynicism, being passed just weeks after France expressed outrage that the NSA had allegedly been engaged in similar activities, at which President François Hollande expressed his "extreme reprobation"[28].

---

[24] Claus Blok Thomsen, Jakob Sorgenfri Kjær, Jacob Svendsen, "Presset FE fortæller om dansk spionage", *Politiken*, November 20, 2013, http://politiken.dk/indland/ECE2138411/presset-fe-fortaeller-om-dansk-spionage/

[25] Draft "EU Human Rights Guidelines on Freedom of Expression Online and Offline", unpublished, version as at November 20, 2013.

[26] Muscio v. Italy, European Court of Human Rights, "Information Note on the Court's case-law No. 102", November 2007, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=002-2419

[27] "Adoption de la loi controversée de programmation militaire", *Le Monde*, December 10, 2013, http://www.lemonde.fr/international/article/2013/12/10/adoption-definitive-de-la-controverse-loi-de-programmation-militaire_3528927_3210.html

[28] Kim Willsher, "French officials can monitor internet users in real time under new law", *The Guardian*, December 11, 2013, http://www.theguardian.com/world/2013/dec/11/french-officials-internet-users-real-time-law

In this way, disclosure of alleged surveillance activities by the NSA and GCHQ is having the effect of ensuring that more of the U.S. and UK's partner nations are ensuring they have the legal framework in place to be able to participate in this activity on an unarguably legitimate basis. Although disclosure of the alleged capability and reach of U.S. and allied surveillance mechanisms prompted strident and outraged reportage in some sections of the English-language media, public opinion has not followed suit. Instead, a more balanced and sober assessment of national security needs is leading European states to pass legislation through due democratic process to ensure that internet monitoring of specific threats to security continues unhindered.

It follows that active measures online in order to prevent and pre-empt threats to national security will continue to be perceived as legitimate despite concerns over privacy, and these measures should be expected to continue unrestrained by the new environment of enhanced public awareness. When Edward Snowden and his associates were considering the likely results of their accusations against the NSA, this is unlikely to have been among their desired outcomes.

Йоко Нитта

Институт национальной безопасности, Япония

Подходы Японии к кибербезопасности Как реагировать на неопределенность?

История вопроса

Когда в 2011 году корпорация Mitsubishi Heavy Industry (MHI) подверглась направленной атаке посредством компьютерного вируса — это стало тревожным сигналом для правительства Японии. Эта компания является крупнейшим в Японии подрядчиком Министерства обороны по поставкам военной техники. А это означает, что MHI обладала сверхсекретной конфиденциальной информацией сил самообороны Японии. Хуже того, MHI не сообщила Министерству обороны о происшедшем, несмотря на то, что есть жесткое требование делать отчёт в подобной ситуации. Это была не просто кибератака, проведенная неизвестными, а ситуация, которая подняла вопрос доверия японского правительства к своим подрядчикам.

Возрастают опасения по вопросу злонамеренного использования киберпространства в деструктивных и вредоносных целях преступниками, террористами, государствами и их агентами. Выросло число и многообразие случаев кибершпионажа, атак на критически важную инфраструктуру, хищения финансов и кибертерроризма. Вопрос кибербезопасности находится в центре внимания Китая и США. В 2010 году использование червя Stuxnet для нарушения работы иранских центрифуг для обогащения урана вызвало опасения по поводу использования неизвестных ИКТ военного назначения в целях «несовместимых с миром и безопасностью». Ввиду сложности атрибуции киберпреступлений, различные акторы безнаказанно используют киберпространство в злонамеренных целях.

Правительство Японии сформировало в кабинете министров Национальный совет по информационной безопасности. Он отвечает за национальную безопасность, а также системы реагирования в чрезвычайных ситуациях. В обязанности Совета входит интерпретация сложных технических

вопросов, преобразование технических и управленческих вопросов в роли и директивы, и координация политического обсуждения новых мер кибербезопасности. Национальный совет по информационной безопасности осуществляет координацию работы министерств, среди которых основными являются: Министерство внутренних дел и связи, Министерство экономики, торговли и промышленности, Национальное полицейское агентство и Министерство обороны. Министерство внутренних дел и связи занимается выработкой политики связи и сетей, Министерство экономики, торговли и промышленности работает над политикой Японии в области информационных технологий, Национальное полицейское агентство борется с киберпреступностью, а Министерство обороны отвечает за национальную безопасность.

На эту новую сферу деятельности также оказывает влияние союз США и Японии. Президент Обама заявил, что США считают киберпространство пятой сферой военного противоборства, и это означает, что США ориентированы на использование кибертехнологий в военных операциях. Япония в этом вопросе последовала по пути США. После выхода в 2012 году доклада Армитажа-Ная, в июне 2013 года правительство Японии опубликовало «Стратегию кибербезопасности Японии».

Среда, в которой находится Япония, значительно изменилась. Слияние киберпространства и физического пространства привело к росту серьёзных рисков, связанных с киберпространством. Кибератаки на государственные учреждения и критические инфраструктуры стали реальностью, мы также приближаемся к состоянию, когда всё будет подключено к Интернету (Интернет вещей) — и эти факторы ускоряют распространение рисков. Кибератаки могут осуществляться из любой точки мира, а киберпространство Японии может быть использовано в качестве плацдарма для нападения в другом месте.

Стратегия Кибербезопасности

Основные принципы Стратегии направлены на создание передового, устойчивого и активного киберпространства, которое необходимо для национальной безопасности и антикризисного управления, социального и экономического развития, и общественной безопасности. Основные принципы направлены на: обеспечение свободного потока информации;

реагирование на все более серьезные риски; развитие подхода, основанного на оценке рисков; совместная партнерская деятельность на основе ответственности каждого. Ключевыми в этой Стратегии являются слова «передовой», «устойчивый» и «динамичный». По этим направлениям были осуществлены следующие основные мероприятия. Для усиления системы безопасности киберпространства Стратегия предусматривает пересмотр стандартов оценки информационной безопасности компьютерных систем центрального правительства. Для развития основ кибербезопасности в Стратегии пересмотрена программа развития человеческих ресурсов в области информационной безопасности. Для развития сотрудничества по основным вопросам киберпространства была создана «Международная стратегия в области кибербезопасности» (j-initiative for Cybersecurity). В декабре прошлого года состоялся Саммит АСЕАН — Япония (2013 г.), на котором обсуждались вопросы сотрудничества в области кибербезопасности. Также в 2015 году планируется расширить круг обязанностей Национального совета по информационной безопасности.

В «Стратегии кибербезопасности Японии» определены три основных направления деятельности. Для обеспечения устойчивости киберпространства, государственных организаций, независимых административных организации и др. усиливается Правительственная группа координации безопасности, которая действует совместно с Мобильной группой помощи при компьютерных инцидентах и Группой реагирования на инциденты, связанные с компьютерной безопасностью. Они проводят совместные учения по реагированию на инциденты, определяют роли соответствующих структур, таких как полиция и силы самообороны, проводят анализ новых угроз, которые появляются вместе с новыми услугами, в том числе социальными сетями и групповой почтой. Развивается обмен информацией между критически важными инфраструктурами, государственными органами, поставщиками оборудования и т.д.; для обеспечения непрерывности бизнеса проводятся межотраслевые учения; создаётся платформа для оценки и проверки систем, в том числе систем управления, используемых в критически важной инфраструктуре, на соответствие международным стандартам. Другие основные направления, выделенные в «Стратегии кибербезопасности», касаются юридических и физических лиц. На малых и средних предприятиях поощряются инвестиции в безопасность, ИТ-предприятиям предоставляются налоговые льготы, если

они через поставщиков Интернет-услуг уведомляют пользователей о заражении вредоносным программным обеспечением и хранят журнал регистрации данных для отслеживания киберпреступлений.

Вторым главным направлением деятельности является обеспечение динамичности киберпространства. В 2011 году Национальный совет по информационной безопасности пересмотрел Программу развития людских ресурсов в области информационной безопасности и Стратегию научно-исследовательских работ.

Третьим направлением деятельности является «Международная стратегия», которая вышла в октябре 2013 года. Стратегия заключается в развитии международного сотрудничества по противодействию уязвимостям, угрозам и атакам в киберпространстве, при участии государственных организаций и национальных Групп реагирования на компьютерные инциденты из таких стран как США, Германия, Великобритания и Япония. Также целью является обмен передовым опытом защиты критической инфраструктуры, обмен информацией о проводимых мероприятиях — например, контактах между правительственными чиновниками, ответственными за защиту критической инфраструктуры, из США, Великобритании, Германии и Японии. Япония планирует сотрудничать по этому вопросу с США, Великобританией, Индией, ЕС и АСЕАН. Принимая участие в соответствующих международных конференциях, Япония вносит свой вклад в процесс выработки правил для киберпространства. Кроме того, осенью 2014 года Япония будет принимать очередную конференцию в рамках процесса Meridian, посвященного защите критически важной инфраструктуры.

Также Стратегия предполагает ежегодный доклад о состоянии кибербезопасности и расширение в 2015 году круга обязанностей Национального совета по информационной безопасности, и его реорганизацию в полноценный Центр кибербезопасности. Для обеспечения работоспособности этой структуры Национальный совет по информационной безопасности, являясь центром сотрудничества между государственным и частным секторами, будет развивать информационную безопасность и, во-вторых, через Правительственную группу координации безопасности отслеживать состояние информационной безопасности министерств и ведомств.

В Японии было выделено 13 секторов критически важной инфраструктуры, и за каждым сектором было закреплено

соответствующее ответственное министерство и связанные организации. Национальный совет по информационной безопасности отвечает за сотрудничество и координацию безопасности критически важной инфраструктуры.

Международная стратегия сотрудничества в области кибербезопасности

Япония осуществляет международное сотрудничество по трём направлениям: способствует развитию общего понимания процессов, участвует в действиях мирового сообщества и способствует глобальному расширению технологических границ.

В Международной стратегии отмечены следующие приоритетные области сотрудничества. В целях быстрого реагирования на киберинциденты Япония создаёт механизмы международного сотрудничества и партнерства для обеспечения глобальных ответных мер — в том числе многосторонний механизм обмена информацией, адекватную систему реагирования на киберпреступления, и концепцию сотрудничества в области международной безопасности в киберпространстве. Для создания основ системы быстрого реагирования Япония продвигает базовые стандарты кибербезопасности и реагирования на глобальном уровне, участвует в создании глобальной системы кибергигиены, продвигает информирование, поддерживает научные исследования в рамках международного сотрудничества. В вопросе выработки международных правил кибербезопасности Япония продвигает разработку международных технологических стандартов и развитие международного нормотворчества для обеспечения стабильного использования киберпространства.

Были расширены и региональные инициативы. Япония тесно сотрудничает с Азиатско-Тихоокеанским регионом, который имеет большое значение по причине географической близости и тесных экономических связей. В этой связи Япония продолжает укреплять отношения с АСЕАН на основе политического диалога, который идёт в рамках Встреч министров АСЕАН-Японии по сотрудничеству в области кибербезопасности, Встреч АСЕАН-Япония по политике информационной безопасности, и Встреч министров АСЕАН-Японии по борьбе с транснациональной преступностью. Эти мероприятия способствуют продвижению таких инициатив, как создание потенциала развития людских ресурсов и осуществление совместных проектов JASPER и TSUBAME. Кроме

этого, Япония будет развивать кибердиалог с Индией. Япония также будет углублять сотрудничество с США на основе японо-американских соглашений по безопасности. Что касается сотрудничества в области кибербезопасности с Европейским союзом, в ноябре 2012 года в Токио состоялась встреча «Япония-ЕС: ИКТ-Интернет» которая стала первой попыткой всестороннего обмена информацией о политических и технологических направлениях развития Интернет-безопасности. Второй форум в формате «Семинара ЕС-Япония по вопросам безопасности ИКТ» состоялся в Брюсселе в декабре прошлого года. Обе стороны обменялись информацией о своих последних политических и технологических мероприятиях, а также обменялись передовым опытом обеспечения безопасности и данными исследований о развитии прогнозирования и быстрого реагирования на кибератаки. Также с 2013 года через Европейскую Седьмую Рамочную Программу осуществляется научно-исследовательское сотрудничество по развитию киберустойчивости. Кроме этого, в Брюсселе, в мае этого года состоялся двадцать второй Саммит ЕС-Япония. В совместном заявлении — «Совместные действия ЕС и Японии в целях глобального мира и процветания» — было подтверждено намерение усилить диалог по вопросам кибербезопасности.

Кибернормы

Что касается глобального партнерства в киберпространстве, Япония признает, что киберпространство является «всеобщим достоянием», как отмечено ГПЭ (группа правительственных экспертов). Япония подчеркивает необходимость выработки общего понимания, как существующие нормы международного права могут применяться в киберпространстве. Важной рекомендацией ГПЭ является то, что «государства должны выполнять свои международные обязательства в отношении приписываемых им международно противоправных деяний» и Япония поддерживает её. Также в докладе ГПЭ рекомендовано принять меры укрепления доверия в киберпространстве, в том числе развивать добровольный обмен мнениями и информацией, создавать двусторонние, региональные и многосторонние площадки, расширять сотрудничество между правоохранительными органами по вопросу реагирования на инциденты. Акцент делается на необходимости развития общего понимания и сотрудничества.

Это важно, так как, по мнению некоторых критиков, учитывая характер угроз в киберпространстве и соответствующие сложности атрибуции, применение международных норм невозможно.

Сейчас интенсивно обсуждается вопрос, нужны ли в киберпространстве международные меры по укреплению доверия и правовые нормы, подобные существующим конвенциям в других областях международной безопасности. Россия, Таджикистан, Китай, Узбекистан, Казахстан и Кыргызстан представили свои проекты договоров для киберпространства. Эксперты приняли это к сведению, но у них до сих пор нет четкого мнения по вопросу необходимости киберконвенции, регулирующей поведение государств в киберпространстве. Это происходит ввиду того, что по вопросу киберконвенции существуют значительные различия в представлениях США с одной стороны и России и Китая с другой. Таким образом, какими бы ни были нормы, с которыми все согласятся, они должны иметь международную легитимность и «благословение» ООН.

Одним из недостатков доклада является то, что в нём нет четких указаний о том, как достигнуть консенсуса по ключевым вопросам кибербезопасности. Дискуссию вызывает даже связанная с киберпространством терминология. Необходимо работать над общим пониманием того, что такое кибервойна, и что подразумевается под применением силы. Для обсуждения технических и правовых вопросов было бы полезно создать полномочный форум ООН, подобный Комитету ООН по мирному использованию космического пространства. К развитию международного права, регулирующего киберпространство, можно привлечь Комиссию по международному праву. При рассмотрении кибервойны, в которой государства или их прокси-агенты осуществляют атаки на критически важную инфраструктуру, важность приобретает вопрос применения силы в киберпространстве. Кибердоктрины некоторых государств предусматривают, что атаки могут вызывать ответную реакцию, которая может не ограничиваться киберпространством. Для понимания того, становится ли киберпространство новой сферой вооруженного противоборства, необходимо проделать значительный объём концептуальной работы. Применимо ли международное право, закрепленное в Женевских конвенциях, к киберпространству? Доклад оставил в стороне эти вопросы и сосредоточился на наименьшем общем знаме-

нателе норм для киберпространства. Это необходимое, но не достаточное условие для обеспечения кибербезопасности.

Ни одно государство не может силой установить свой суверенитет в киберпространстве. Однако это осуществимо, если каким-либо образом заявить территориальные притязания в киберпространстве. Например, Япония является островным государством и её возможности по международной телефонной связи на 95% зависят от подводных кабелей. Таким образом, можно считать, что суверенитет Японии начинается у места выхода подводного кабеля на берег.

Независимо от того, кто является владельцем сервера, гражданин Японии, или иностранец — можно полагать, что если вещество или материал находится в Японии, то он относится к Японии. Предположим, что суверенитет Японии распространяется таким образом. Это согласуется с ситуацией, когда иностранцы, если они совершают преступления в Японии, получают наказание. Правительства Японии, США и Австралии считают, что свобода информации и Интернет-свобода являются критически важными и должны обеспечиваться. Следует избегать чрезмерного вмешательства правительств в киберпространство. С 1990-х годов, когда Интернет был воспринят многими людьми, существующее состояние свободы является наиболее значимым аспектом, и мы должны не утерять его. Таким образом, эти государства пытаются избежать обсуждения вопросов только в рамках ООН и стараются следовать многостороннему подходу, при котором, как ожидается, вопросы, связанные с киберпространством, будут обсуждаться многими акторами.

В 2015 году в Гааге состоится Конференция по киберпространству а в 2014 году продолжит работу ГПЭ ООН. Необходимо следить за ситуацией и понять, сможем ли мы добиться результата, или решение вопросов вновь будет отложено на потом.

Выводы

В различных документах Правительства США продвигается линия, что киберпространство следует признать «всеобщим достоянием». Всеобщее достояние — это пространство, которое не может находиться под контролем одной страны, и от которого зависят все государства.

Однако киберпространство является совокупностью серверов, линий связи, систем хранения информации и т.д., и

киберпространство невозможно рассматривать как обычное всеобщее достояние. Если оно рассматривается как совокупность оборудования, то киберпространство в значительной степени уязвимо к частичному или полному разрушению.

Причина, по которой все страны рассматривают этот вопрос, заключается в том, что сейчас вооруженные силы и экономика сильно зависят от киберпространства. Киберпространство является пятой сферой вооруженного противоборства, но в то же время скорее является гибким связующим звеном между четырьмя другими — сушей, морем, воздухом и космосом, и способствует деятельности человека.

Характерной особенностью проблемы управления киберпространством является то, что управление успешно развивалось самостоятельно, но когда правительства попытались вмешаться, этот вопрос перешёл в политическую плоскость. Инженеры часто говорят: «работает — не трогай». На протяжении последних десятилетий идёт обсуждение вопроса, что такое управление Интернетом, и работает оно, или нет. Сейчас, когда вопросы безопасности становятся все более важными, и необходимо стабильное и безопасное управление, обсуждения должны быть прекращены. Государственное управление киберпространством, на котором настаивает Россия и Китай, изменит существующую систему управления. Следствием этого может быть утрата созданного киберпространством динамизма.

Сейчас мы должны позаботиться о том, чтобы киберпространство осталось всеобщим достоянием, признать его уязвимость и повысить его безопасность. Важно обеспечить безопасность физической инфраструктуры, поддерживать свободный поток информации, и развивать правила, связывающие их воедино.

Использованная литература

1. National Information Security Council “Japan Cybersecurity Strategy” June 13, 2013 http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf

2. National Information Security Council “International Strategy on Cybersecurity Cooperation ~ J-initiative for cybersecurity” October 2013 http://www.nisc.go.jp/active/kihon/pdf/InternationalStrategyonCybersecurityCooperation_e.pdf

3. The Government of Japan “National Security Strategy of Japan” December 2013 http://www.cas.go.jp/jp/siryou/131217anzenhoshou/nss-e.pdf

4. Center Strategic for International Studies “The Armitage-Nye Report: U.S.-Japan Alliance: Anchoring Stability in Asia”: August 2012 http//csis.org/event/us-japan-alliance-anchoring-stability-asia

5. Joint ministerial statement of the Asean-Japan ministerial policy meeting on Cybersecurity Cooperation, Tokyo, 13 September 2013 http://www.meti.go.jp/press/2013/09/20130913005/20130913005-5.pdf

6. MERIDIAN Connecting an Protecting previous conference, Meridian 2013, Buenos Aires http://meridianprocess.org/cms.aspx?e=21&id=6&cg=a4cab139-a2b6-4789-bed5-bb106880674d

Yoko Nitta
National Security Institute, Japan

Japan's Approaches towards Cybersecurity

How to respond to uncertainty?

Background

It was a wake-up call for Japanese government when Mitsubishi Heavy Industry (MHI) got virus infection by targeted attacks in 2011. The industry is the biggest contractor of Ministry of Defense (MOD) for defense equipment in Japan. Which means MHI has dealt with the top-level confidential information for Japan's armed force defense. To make things matter worse, MHI did not report what happened to MOD although there is a strict regulation for report under that condition. It did not stay only as a cyber attack from the unknown but it pointed Japanese government the trust matter with their contractors.

Concerns have grown over the misuse of cyberspace by criminals, terrorists, states and their proxies for disruptive and malicious activities. Cases of cyber espionage, attacks on critical infrastructure, financial thefts and cyber terrorism have grown manifold. Cyber security has become a high-profile issue between China and the US. The use of the worm Stuxnet in 2010 to disrupt Iranian centrifuges being used for uranium enrichment has raised concerns about undeclared cyber warfare ICTs are being used for purposes that are "inconsistent with national peace and security". Attribution of cyber crime being a difficult exercise, the actors misuse cyberspace with impunity.

Japanese government set up National Information Security Council (NISC) within Cabinet Office before that. NISC has dual responsibilities of national security and emergency response systems. The responsibility of NISC is supposed to interpret complicated technical issues, transform of technical and managerial issues into poles and directives and coordinates the political debate concerning emerging cyber security measures. NISC coordinate ministries, main ministries are : the Ministry of Internal Affairs and Communication (MIC), the Ministry of Economy, Trade and Industry (METI), the National Police Agency (NPA), and the Ministry of

Defense(MOD). MIC deals with communication and network policies, METI works on Japan IT polices, NPA deals with fighting cyber crimes and MOD is responsible for national security.

Plus US- Japan alliance gives a impact on this new dimension and Japan has followed its US direction for since the US President Obama already made an announcement that US regard cyber as the domain of fifth war, which means US focuses on the use of cyber technologies military operations. Followed by the pressure Armitage — Nye report published in 2012, Japanese government launched 'Japan Cybersecurity Strategy' in June 2013.

Also, environment surrounded Japan has changed dramatically in terms of cyberspace and real- space have been merged and integrated which has increased serious risks surrounding cyberspace. Cyber attacks against government institutions and critical infrastructures have become a reality, advent of conditions where everything is connected to the internet (Internet of Things) have increased the spread of the risks, cyber attacks can be effaced from anywhere in the world, and carried out in cyberspaces affiliated with Japan as a springboard for attacks elsewhere.

Cybersecurity Strategy

Basic principles of the strategy constructs a world-leading, resilient and vigorous cyberspace for national security/ crisis management, social/economic development, and safety/security of public. Main pillars of the basic principles are to ensure free flow of information, to respond to increasingly serious risks, to enhance risk-based approach, to act in partnership based on shared responsibilities. The key words of the strategy are 'Resilient', ' Dynamic', ' World-Leading'. Japan main recent efforts based on these key words are the following: To strengthen protection for cyberspace, the strategy revises of the Standards for Information Security Measure for the Central Government Computer Systems, To build fundaments, the strategy revises the information security human resource development program, world-leading cyberspace issues international strategy on cybersecurity cooperation ~ j-initiative for cybersecurity~, ASEAN — Japan Commemorative Summit Meeting was held last December (2013), and to strengthen the function of NISC is scheduled in 2015.

Japan 'Cybersecurity Strategy' lays out the three main efforts. For Resilient Cyberspace, Government Organizations, Independent Administrative Organizations, etc. plays a role as strengthening Government Security Operation Coordination team (GSOC), accurate and quick response through cooperation Cyber Incident

Mobile Assistant Team (CYMAT)and CSIRT, conducting incident response drills, specifying roles of related organizations such as the police and the Self Defense Forces, to measure for new threats pursuant to new services, including Social Network Service (SNS) and group mail. Critical Infrastructures Industries strengthen information sharing with government organizations and system vendors, etc., executing cross-sector exercises for ensuring business continuity, build a platform for evaluation and authentication of such systems as control systems used by critical infrastructure, in compliance with international standards. The other main efforts based on the 'Cybersecurity Strategy ' is dealt with by enterprises and individuals. They promote investment in security by small and medium-sized businesses, through incentives sun as tax systems, to measure by IT-related businesses including notifying malware infection to individuals by ISPs and to ensure the traceability of cyber crimes, such as by examining the way to store logs.

The second main effort is to get the fundamentals for Dynamic Cyberspace. Information Security Policy Council revised the Information Security Human Resource Development Program and its Research and Development Strategy in 2011.

The third effort is to have launched 'International Strategy' last October 2013. The strategy is to promote international measures related to vulnerabilities, threats, and attacks in cyberspace with the participation by government organizations and CSIRTS from countries such as the US, Germany, the UK and Japan. Also it is aims at sharing best practices for the protection of critical infrastructure, exchanging information on measures such as international cooperation with participation by government officials in charge of protecting critical infrastructure from countries such as the US, the UK, Germany and Japan. Japan is going to cooperation on this issue with US, UK India, EU and ASEAN. Japan contributes international rule making in cyberspace attending the related international conferences. Plus, Japan is going to host MERIDIAN this coming autumn.

Also the strategy issues annual report on cybersecurity and strengthens the function of NISC scheduled in 2015 to become fully its operations, renaming as Cyber Security Center. Japanese government will aim for the new system to become fully operations. In this regard, NISC is to promote information security as a hub of cooperation between the public and private sectors and to cross-monitor the information security status of ministries and agencies through the Government Security Operation Coordination (GSOC) team.

Thirteen sectors have been incorporated as the ones to be focused as critical infrastructure in Japan and the specific miniseries and its related organization are to responsible for each field. NISC is to coordinate and cooperate for the critical infrastructure.

International Strategy on Cybersecurity Cooperation

Three directions of Japan's contrition for strengthening international cooperation are: Incremental fostering of common global understanding, Japan's contraption to the global community and expansion of the technological frontier at the global level.

The priority areas of the international strategy are the following: for implementation of dynamic responses to cyber incidents, Japan builds a mechanism for international cooperation and partnership for global responses to expanding cyberspace such as enhancing multilayered mechanism for information sharing, working on appropriate response to cyber crime and establishing framework of cooperation for international security in cyberspace. For building up " fundamentals" for dynamic response, Japan raises the cybersecurity standard of basic capability and response mechanisms at the global level supporting for building a global framework for cyber hygiene, promoting awareness-rapid activities, enhancing research and elopement through international cooperation. For international rule making for cybersecurity, Japan promotes international rule making for ensuring stable use of cyberspace formulating international standards of technology and pursuing international rule making.

Japan's regional intiatives have been enhanced; for the Asia Pacific, Japan has cooperated closely with Asia Pacific region, which is crucial due to geographical proximity and close economic ties. In this regard, Japan will have continued to strengthen the relationship with the ASEAN through policy dialogues as ASEAN-JAPAN Ministerial Meeting on Cybersecurity Cooperation, ASEAN-Japan Information Security Policy Meeting, and ASEAN-Japan Ministerial Meeting on Transnational rime, promoting initiatives such as capacity building for human resources development and promoting joint projects such as JASPER and TSUBAME. Plus, Japan will promote Japan-India cyber dialogue. Japan will deepen partnership with the U.S. centered on the Japan-U.S. Security arrangements. Regarding EU-Japan cooperation on cyberseucrity, "Japan-EU ICT Internet" was held in Tokyo in November 2012 as a first attempt to comprehensively exchange information on policy and technology trends of internet security. The second forum was held

as "EU-Japan ICT Security Workshop" in Brussels last December. Both sides updated their recent policy and technology measures as well as exchanged good practices as ICS (industrial Control System) security and R&D on trend foresting / quick response to cyber attacks. Joint R&D cooperation for improving cyber-resilience has been also promoted through FP7 since 2013. Also this May, twenty second EU- Japan Summit was held in Brussels. In the Joint press statement, " The EU and Japan Acting together for Global Peace and Prosperity", it reforest to their decision to launch cyber dialogue.

Cyber Norms

Regarding global partnership in cyber space, Japan recognizes cyberspace as "global commons" in GGE(Group of Governmental Experts). It stresses the need for a common understanding on how norms based on existing international law could be applied in cyberspace. The critical recommendation made by the GGE is that "States must meet their international obligations regarding internationally wrongful acts attributable to them" and Japan supports it. Also the reports UN submitted goes on to recommend confidence-building measures in cyberspace such as voluntary exchange of views and information sharing, creation of bilateral, regional and multilateral frameworks, increased co-operation on incident response and synergy among law enforcement agencies. The emphasis is on the need to enhance common understanding and co-operation.

This is important considering several critics hold that given the nature of threats in cyberspace where attribution is difficult, the application of international norms may not be possible.

There has been intense debate whether cyberspace also requires international cyber security confidence-building measures and rules on the lines of similar conventions in other areas of international security. In fact, countries like Russia, Tajikistan, China, Uzbekistan, Kazakhstan and Kyrgyzstan have come out with drafts for cyberspace. Experts take note of this but do not take a clear view whether a cyber convention to govern states' behaviour in cyberspace is needed. This is because there are considerable gaps in the thinking of the US on one hand and Russia and China on the other with regard to a cyber convention. It implies that whatever norms are agreed upon must have international legitimacy and UN blessing.

One weakness of the report is that it does not offer clear guidance on how to build consensus on key cyber security issues. In cyberspace, even the vocabulary is contentious. A common understanding of issues such as what is cyber warfare and what implies the use of force needs to be developed. It would be useful to set up a UN mandated forum, much like the UN Committee on the Peaceful Uses of Outer Space, to deliberate on technical and legal issues. The International Law Commission could also be involved to develop the international law governing cyberspace. In the context of cyber warfare, involving attacks on their critical infrastructure by states or proxies, use of force in cyberspace becomes important. The cyber doctrines of some states stipulate that attacks would elicit response that may not be confined to cyberspace. A lot of conceptual work still needs to be done to understand if cyberspace is emerging as a new arena of warfare. Does the international law codified in Geneva Conventions apply to cyberspace? The report has skirted these issues and focused on the lowest common denominator of cyber norms. This is necessary but not a sufficient condition to ensure cyber security.

Any counties cannot force its sovereignty to cyberspace. However, it will be possible to enforce that if they can claim her territory in some ways in cyber space. For instance, Japan is an island country and her capacity of international telecommunication relies on marine cable up to 95%. Therefore, it is possible to regard the part from landing station of marine cable is the domain of Japan's sovereignty.

No matter he/ she is foreigner, server belong to non-Japanese, it would be simple to think if the substance or the material located within Japan belongs to Japan. Suppose Japan's sovereignty extends to. This aligns with the case that foreigners get punished in Japan if they commit the crime here. The government of Japan, U.S. and Australia regards free flow of information, internet freedom, is a critical value and should be ensured. Excessive intervention by the government to cyber space should be avoided. It is indeed the most crucial part since 1990's when internet has been accepted by many people and we should not lose that. Therefore, they try to avoid discussion only within U.N. and have tried to pursue multi-stakeholder approach in which they expect diverse actors to discuss the cyber issues.

Cyber space convention will be held at Hague in Netherlands in 2015 and GGE will re-start in 2014. We need to monitor whether we could get the result by then or take a rain check, which is a situation for a time being.

U.S. government has insisted that cyber space should be recognized as " global commons " in their various reports. Global commons is the remain which one country cannot control but every countries rely on its area.

However, cyber space is just an accumulated of telecommunication servers, lines and memory tips, etc, and it is not appropriate that cyber space should be viewed as the conventional global commons. If it is seen as an accumulated ones of equipment, cyber space is quite vulnerable and partial breakdown or collapse.

The reason why each countries stick to this issue is because military and economy strongly relies on cyber space now. Cyber space is the fifth domain of warfare but it rather connects the other four fields, land, sea, air and space, smoothly and facilitates human activities.

The governance of cyber space is different because it used to go well but government tried to intervene and it became a political issue. Engineers often say that `If it ain't broke, don't fix it.' Whether internet governance is broken or not and the definition of it has discussed for the past decades. Now that security issues are getting more serious and stable and safe governance is in need and discussion should be curbed. The state-led cyber space management that Russia and China has insisted will change the course of conventional governance to government and it is possible to lose its dynamism which cyber space bas produced.

Now we need to make sure that the cyber space is a global common and recognize its vulnerability and should enhance its security. Keeping physical infrastructure, seeking for free flow of information as contents and developing the rule setting to connect them is essential.

Bibliography

1. National Information Security Council "Japan Cybersecurity Strategy" June 13, 2013 http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf

2. National Information Security Council "International Strategy on Cybersecurity Cooperation ~ J-initiative for cybersecurity" October 2013 http://www.nisc.go.jp/active/kihon/pdf/InternationalStrategyonCybersecurityCooperation_e.pdf

3. The Government of Japan "National Security Strategy of Japan" December 2013 http://www.cas.go.jp/jp/siryou/131217anzenhoshou/nss-e.pdf

4. Center Strategic for International Studies “The Armitage-Nye Report: U.S.-Japan Alliance: Anchoring Stability in Asia”: August 2012 http//csis.org/event/us-japan-alliance-anchoring-stability-asia

5. JOINT MINISTERIAL STATEMENT OF THE ASEAN-JAPAN MINISTERIAL POLICY MEETING ON CYBERSECURITY COOPERATION Tokyo, 13 September 2013 http://www.meti.go.jp/press/2013/09/20130913005/20130913005-5.pdf

6. MERIDIAN Connecting an Protecting previous conference, Meridian 2013, Buenos Aires http://meridianprocess.org/cms.aspx?e=21&id=6&cg=a4cab139-a2b6-4789-bed5-bb106880674d

Масаеси Кубоя
Университет Токай, Япония

Доверие к киберпространству в Японии: Информационная грамотность и регулирование

1. ИКТ и их негативное влияние на детей: причины беспокойства японцев.

В середине 1980-х годов компьютеры получили широкое распространение в Японии. Что касается среднестатистических японских семей, в их домах первыми компьютерами были видеоприставки. Разработчик игр, компания Nintendo, создала широко известную игровую приставку «Family Computer» (семейный компьютер).

Негативное влияние ИКТ на молодое поколение стало серьезной социальной проблемой. Многие родители в Японии говорили: «Не играйте в видеоигры», или «Реальная жизнь не может быть перезапущена, реальная жизнь отличается от виртуального мира игры». В 1980-х и 1990-х годах этот вопрос был серьезной общественной проблемой. Целью настоящей статьи является исследование того, как в Японии развивалось доверие к киберпространству.

2. Ответственность родителей за использование сети Интернет молодёжью

Несмотря на то, что в настоящий момент существует определенное регулирование рынка видеоигр, проблема правильного использования игровых консолей во многом лежит на родителях. Система регулирования в Японии является неправительственной и саморегулируется отраслью. Игровая индустрия Японии создала Рейтинговую организацию компьютерных развлечений, которая ввела добровольную систему регулирования.

Когда эта система была создана игровой индустрией в Японии в 2002 году, подобные системы регулирования уже были внедрены в западных странах. Например, в Великобритании система регулирования была введена уже в 1980-е годы. США, Франция и Германия создали свои системы в 1990-х годах.

В Великобритании правовое регулирование и саморегулирование объединены. Правительство США приняло закон, в котором говорится: «если промышленность не создаст свою собственную добровольную систему регулирования за год, правительство США введёт правовую систему». Это привело к быстрому созданию саморегулирования.

В Японии нет подобных правовых предпосылок или правительственных инициатив. Кроме того, изначально японская промышленность не хотела иметь такую систему регулирования, и против своей воли ввела систему по зарубежному образцу. В результате, более предпочтительным методом самоограничения стал родительский контроль.

3. Доверие к Интернету в Японии

Есть два способа обеспечения доверия к Интернету. Первый способ является механическим и техническим. Этот метод, как правило, предполагает внедрение системы фильтрации и предотвращает доступ людей к вредоносной информации.

Этот метод является очень действенным в качестве услуги для мобильных телефонов. Когда родители покупают своему ребёнку сотовый телефон, они должны сообщить персоналу магазина возраст пользователя. После этого активируется мощная система фильтрации, предоставляемая оператором сотовой связи. Пожалуй, во всех японских мобильных телефонах для детей[1] есть мощная система фильтрации, которую дети не могут самостоятельно отключить. В случае домашних компьютеров этот метод по-прежнему является действенным, потому что родители могут контролировать поведение детей, когда сидят рядом с ними.

К сожалению, другие мобильные устройства, в том числе смартфоны, мобильные компьютеры и планшеты трудно

---

[1] Японские мобильные телефоны иначе называются «Галапагосскими» — в честь изолированных от континентов островов, находящихся в юго-восточной части Тихого океана, на которых шли уникальные эволюционные процессы. До того, как в мире распространение получили смартфоны, операторы мобильной связи Японии разработали многофункциональные мобильные телефоны, через которые посредством серверов и сети сотового оператора можно было получить доступ в Интернет. Вкратце, экраны этих телефонов меньше, чем у смартфонов, и администраторам веб-страниц приходится делать отдельный вариант страниц для этих телефонов. С ростом популярности смартфонов в Японии, количество пользователей обычных мобильных телефонов постепенно снижается.

контролировать. Эти устройства, как правило, имеют беспроводное соединение Wi-Fi, и дети могут получить доступ к Интернету, минуя сети оператора мобильной связи. Конечно, когда дети используют эти устройства, родители не всегда могут сидеть рядом и наблюдать за ними. Необходимо отметить, что в эпоху смартфонов фильтрация не может быть всеохватывающей.

Второй способ реализуется через человека, развитие способностей людей — особенно, информационной грамотности. Существующий в японской правовой системе «Закон о развитии среды, обеспечивающей безопасное и защищенное использование Интернета молодёжью» требует, чтобы каждый человек или организация, которая владеет веб-сайтом, назначала «уполномоченного администратора серверов», в обязанности которого входит наблюдение за тем, что сайт не содержит вредоносной информации.

Помимо правовых требований, японское правительство попыталось обучить детей, чтобы они были осведомлены и могли справиться с различными рисками в Интернете. В качестве первого шага, правительство оценило возможности и навыки молодежи в области ИКТ, для разработки Индикатора оценки Интернет-грамотности студентов.

В рамках этой оценки проводится измерение нескольких навыков, в том числе следующих трех: решение проблем, связанных с незаконным и вредоносным контентом; адекватное общение в Интернете; защита конфиденциальности и использование адекватных инструментов обеспечения безопасности. Эти навыки нужны не только детям, взрослые также должны их получить. И мы таким образом можем утверждать, что Индикатор оценки Интернет-грамотности студентов полезен и для измерения грамотности во всей стране.

На международном уровне Индикатор оценки Интернет-грамотности студентов является новаторским направлением развития информационной грамотности молодёжи. Продвигая его, правительство Японии содействует международному обществу.

4. Политика информационной грамотности в Японии на местах

Некоторые местные органы власти также пытаются повысить информационную грамотность людей. Например, правительство префектуры Ибараки назначает инструкторов для

преподавания медиа-грамотности. Эти инструкторы проводят семинары для родителей, чтобы объяснить им, что они несут основную ответственность за безопасное использование Интернета своими детьми. Хотя преподаватели часто проводят семинары для детей и преподают им напрямую, они в приоритетном порядке проводят семинары для родителей до или после семинаров для детей. Это позволяет подчеркнуть ответственность родителей.

Второй пример из города Сока. Муниципальное правительство требует участия администраторов серверов в учебной программе, проводимой некоммерческой организацией (НКО). Эта организация выдает сертификат, что администрация города назначает в качестве ответственных за поддержание своих веб-сайтов должным образом подготовленных специалистов.

5. Деятельность японских некоммерческих организаций в области информационной грамотности

Вот некоторые примеры деятельности НКО по продвижению информационной грамотности:

- IAJapan (Интернет-общество Японии) участвует в разработке систем фильтрации;
- EMA (Ассоциация оценки и мониторинга контента) оценивает сайты для мобильных устройств;
- I-ROI (Исследовательский институт оценки Интернет-ресурсов) выдает сертификаты для самостоятельной оценки контента;
- JISPA (Японская ассоциация продвижения Интернет-безопасности) распространяет среди администраторов веб-сайтов руководства по самостоятельным действиям.

Рассмотрим более подробно деятельность Исследовательского института оценки Интернет-ресурсов. В 2013 году он запустил программу Экспертов в области цифрового контента (DCA). Эта программа специализируется на безопасном использовании Интернета и является не технически, а социально-ориентированной. Программа разделена на три уровня: пользователя, администратора и инструктора. Уровень 2 DCA (администратора) соответствует «уполномоченному администратору серверов», о котором говорится в «Законе о развитии среды, обеспечивающей безопасное и защищенное использование Интернета молодёжью».

Участникам программы DCA дают глубокие профессиональные знания по безопасному использованию Интернета, которые охватывают не только использование Интернета детьми, но также и взрослыми. Примечательным моментом программы DCA Исследовательского института оценки Интернет-ресурсов является сотрудничество со школами и университетами. Сертификат DCA третьего уровня (пользователя), может быть получен студентами после прохождения ими специальных занятий в колледже.

Таким образом, программа DCA Исследовательского института оценки Интернет-ресурсов использует подход, ориентированный на общество и человека, и, выдавая сертификаты лицам, имеющим соответствующие знания, способствует развитию образования человеческих ресурсов. Если в программе DCA Исследовательского института оценки Интернет-ресурсов примет участие множество людей, и они получат сертификаты DCA, эта программа будет высоко оценена общественностью. А затем, когда люди увидят на каком-либо сайте знак Исследовательского института оценки Интернет-ресурсов, они будут уверены, что сайт является безопасным и надежным, и благодаря этой отметке люди смогут оценить уровень безопасности веб-сайта.

Если мы сможем претворить эту идеальную ситуацию в жизнь, то сможем развивать доверие к Интернету.

6. Некоторые тезисы

В заключение, я хотел бы задать несколько вопросов.

Во-первых, что должно иметь приоритет — безопасность или свобода? Как уже было сказано выше, политика правительства и законы Японии в основном ориентированы на использование Интернета детьми. Должны ли мы также обратить внимание на использование Интернета взрослыми людьми? Должно ли правительство ограничивать их свободу слова? В настоящее время, даже применительно к детям, существующее в Японии правовое требование звучит не как «обязательство», а «обязательство приложить усилия».

Следующий тезис: «Что должны делать правительства?» Введение Индикатора оценки Интернет-грамотности студентов — это хорошая работа, и она будет содействовать дальнейшему обсуждению. Однако, это всего лишь индикатор для проведения анализа. Итак, нужна ли нам какая-то другая политика или метод развития доверия к Интернету? Или в большей степени доверять людям или НКО, чем правительству?

Эти вопросы можно перефразировать: «Что является более предпочтительным, государственное регулирование, обучение родителей или деятельность НКО?» На мой взгляд, развитие образования и социальный консенсус лучше, чем государственное регулирование. На самом деле, японское центральное правительство неоднократно рекомендовало местным органам власти: «Не создавайте руководящие принципы сами, обращайтесь к НКО».

Есть пример, когда столичный муниципалитет Токио пытался создать руководящие принципы самостоятельно. В ответ на это правительство страны отдало приказ о принудительном исполнении. В приказе было сказано, что национальные и местные органы власти должны уважать роль НКО. Задача центрального правительства заключается в том, чтобы продвигать деятельность НКО, и при этом минимизировать государственное участие.

Последний вопрос: «Использовать технически-ориентированный или социально-ориентированный подход?» Как уже было сказано выше, осуществлять фильтрацию Интернета и других виртуальных сетей становится все труднее и труднее. Поэтому я полагаю, что в ближайшем будущем важность социально-ориентированного подхода, безусловно, увеличится. На самом деле, одно должностное лицо заявило, что несколько лет назад, при рассмотрении системы фильтрации, никто не принимал во внимание смартфоны. Это означает, что технически-ориентированный подход должен идти в ногу с новыми технологиями, а это очень трудно сделать.

Конечно, социально-ориентированный подход находится только в начале пути. Как я уже отметил выше, программа DCA Исследовательского института оценки Интернет-ресурсов пытается претворить в жизнь «идеальную ситуацию» и развивать таким образом доверие к Интернету. Я знаю, что это не так просто сделать. В течение некоторого времени технически-ориентированные и социально-ориентированные подходы будут существовать параллельно.

Dr. Masayoshi Kuboya
Tokai University, Japan

Cyberspace Credibility in Japan: Information Literacy and Regulation

1. *ICT and its negative impacts on children: Why Japanese worry*

In the mid 1980s, computers became widespread in Japan. As for average Japanese families, video consoles were the first computer in their houses. Game software manufacturer Nintendo made the iconic game console and called it the "Family Computer".

ICT's negative impacts on the young generation became a serious social issue. Many Japanese adults said, "Don't play with video games", or "Real life cannot be reset, real life is different from the virtual game world". This kind of argument was a major concern in the society in the 1980s and 1990s. This brief paper seeks to explore how Japan has developed its cyberspace credibility.

2. *Parental Responsibility for Young People's Internet Use*

Although there are today some regulations on video games, the proper use of game consoles largely relies on parents. Japan's regulation system is not governmental but self-regulated by the industry. Japan's game industry launched CERO, Computer Entertainment Rating Organization, which introduced the voluntary regulation system.

When the system was established by the game industry in Japan in 2002, similar regulatory systems had already been enforced in western countries. For example, the UK had introduced their regulation system as early as the 80s. USA, France and Germany built up their systems in the 1990s.

In the UK, legal regulation and self-regulation are combined. The US government enacted a law, which stated: "if the industry does not build up its own voluntary regulatory system in a year, the US government will enforce a legal system". This led to a prompt installation of self-regulation.

In Japan, such a legal, or governmental, background cannot be found. In addition, the Japanese industry did not want to have such regulations at first and reluctantly imported the system from

overseas. As a result, parental guide as a self-restraint has come to be preferred.

3. *Internet Credibility in Japan*

There are two ways to ensure internet credibility. The first method is mechanical and technical. This method usually enforces a filtering system and prevents people from having access to malicious information.

As a feature for mobile phones, this method is very powerful. When parents buy a cell-phone for their child, they have to tell the user's age to retail shop staff. So they can activate a strong filtering system, which is provided by the mobile phone carrier. All children's Japanese style feature phones[1] seem to have strong filtering systems which children cannot deactivate by themselves. In the case of home computers, the method is still powerful because parents can monitor children's behavior when they sit beside them.

Unfortunately, other mobile devices, including smart phones, mobile pcs and tablets, are difficult to control. These devices usually have a wi-fi system, and children can access the internet without passing through a mobile phone carrier network. Of course, parents cannot always sit beside and monitor them when their children use these devices. We have to notice that filtering cannot cover all in the era of smart phones.

The second method is a human way. This method tries to facilitate people's ability, especially information literacy. In the Japanese legal system, the "Act on Development of an Environment that Provides Safe and Secure Internet Use for Young People" requires that every person or organization which owns a website must make an effort to assign a "specified server administrator", who must oversee that the website does not contain harmful information.

Apart from legal requirements, the Japanese Government has tried to instruct children to be able to deal with various risks on the internet. As a first step, the Government has assessed youngsters'

[1] Another name of "Japanese style feature phone" is "Galapagos mobile phone". "Galapagos" comes from the islands in South-eastern Pacific Ocean, which is totally isolated from any continents and whose evolution process is very unique. Before smart phone became widespread in the world, Japanese mobile phone companies had developed the multi-functional mobile phones which can access to the internet through mobile phone carriers' servers and networks. Briefly speaking, these phones' screens are smaller than smart phones and website administrators have to make a specific webpage just for these phones. After smart phones got popularity in Japan, the number who uses Japanese style feature phones has been gradually decreasing.

ICT capabilities and skills, to develop a measurement called the Internet Literacy Assessment Indicator for Students (ILAS).

ILAS tries to measure several competencies, including the following three; to deal with the problems of illegal and harmful contents, to communicate adequately on the internet, and to protect privacy and use adequate security instruments. These competencies are not only for children and should be acquired of adults, too. Then, we can say that ILAS is also useful for measuring national literacy.

At the international level, ILAS is a pioneering work for young people's information literacy. The Japanese Government is trying to contribute to international society by promoting this indicator.

4. *Local Policies on Information Literacy in Japan*

Some local authorities also try to facilitate people's information literacy. For example, the Ibaraki prefectural government designates media education instructors. These instructors hold seminars for parents to teach them that they are most responsible for their children's secure internet use. Although the instructors may often hold seminars for children and teach them directly, they organize seminars for parents as a priority to be held before or after the seminars for children. In this manner, parents' responsibility is also emphasized here.

The second case involves Soka city. The municipal government requires its server administrators to participate in a training program conducted by a non-profit organization. The NPO issues a certificate stating that the city office designates properly-trained persons in charge of maintaining its websites.

5. *NPOs on Information Literacy in Japan*

These are some examples of NPO activities promoting information literacy:

- IAJapan (Internet Association Japan) engages in developing filtering systems.
- EMA (Content Evaluation and Monitoring Association) evaluates mobile sites.
- I-ROI (Internet-Rating Observation Institute) issues certificates for self content assessment.
- JISPA (Japan Internet Safety Promotion Association) promotes self-guideline for website administrators.

Here I focus on I-ROI's effort. I-ROI launched the Digital Contents Assessor (DCA) program in 2013. The DCA assessor

has competencies about secure internet use. The competencies are not technically-oriented but socially-oriented. DCAs fall into 3 categories; user, administrator and instructor levels. A DCA level 2 administrator level personnel corresponds to the "specified server administrator" in the "Act on Development of an Environment that Provides Safe and Secure Internet Use for Young People".

In the DCA program, adequate competencies for secure internet use are taught. The competencies focus on not only children's internet use but also adults' internet use. A notable fact of I-ROI's DCA program is collaboration with schools and universities. DCA level 3, the user level, certificate can be granted to students through designated college classes.

That is, I-ROI's DCA program employs a socially-oriented, human-oriented approach, engaging in education of human resources, to issue certificates to persons who have proper knowledge. If many people take I-ROI's DCA programs and declare that they have DCA certificates, the DCA program will be well acknowledged by the general public. And then, when people find an I-ROI mark on some website, they can be confident that the site is safe and reliable. People can evaluate the safety level of a website by the I-ROI mark shown on the site.

If we can make this ideal situation come true, we can develop the credibility of the internet.

6. *Some Arguments*

To conclude, I will ask some questions.

The first one is "which should be prioritized, safety or liberty?" As I mentioned above, Japanese Governmental policies and laws largely focus on children's internet use. Do we need to focus on adults' use too? Should the government constrain adults' freedom of speech? As of now, even for children, the Japanese current legal requirement is not "obligation" but "obligation to make an effort".

The next argument is "what should governments do?" ILAS is a good work and it will facilitate discussions. However, this is just an indicator for analysis. So, do we need some other policy or method to develop internet credibility? Or, do you trust people or NPOs more than the government?

These questions can be rephrased: "Which is to be preferred, governmental regulation, parental education or NPO activities?" In my view, education and social consensus are better than governmental regulation. In fact, the Japanese national government

has repeatedly recommended to local governments: "Do not make guidelines by themselves, refer to NPO".

In the case of the Tokyo metropolitan government, it tried to make its guideline by itself. In response, the national government has given an enforcement order. The order says that national and local governments should respect the role of NPOs. The purpose is that the national government wants to promote NPO's activities while minimizing governmental involvement.

The last question is "technically-oriented approach or socially-oriented approach?" As I mentioned above, it is getting harder and harder to filter the internet and other virtual networks. Therefore, I think the importance of the socially-oriented approach will definitely increase in the near future. Actually, a public official pointed out that nobody took account of smart phones when considering the filtering system a few years ago. This means the technically-oriented approach needs to keep up with new technologies, which is very difficult to do.

Of course, the socially-oriented approach has just reached the starting line. As I noted above, I-ROI's DCA program tries to make "ideal situation" come true to develop the credibility of the internet. I know it is not easy to make this ideal situation come true. Both technically-oriented and socially-oriented approaches will live side-by-side for a while.

Н.П.Варновский, О.А.Логачев, В.В.Ященко

Институт проблем информационной безопасности
МГУ имени М.В.Ломоносова

Математика и информационная безопасность

Что надо нам, того не знаем мы,
Что знаем мы, того для нас не надо.

— Иоганн Вольфганг фон Гёте. «Фауст»

Информационная безопасность — весьма популярная тема. Поисковые системы дают для этого термина сотни миллионов ссылок на ресурсы V^6 (= W^3 = WWW). Однако, если к термину «информационная безопасность» добавить слово «математика», то это количество снижается на порядки. Это отчасти отражает преобладающее мнение, что информационная безопасность представляет собой организационно-техническую задачу, а не научную проблему. Так что роль математики ограничена обеспечением таких методов, как шифрование данных, используемых в качестве строительных блоков для систем информационной безопасности.

Это серьезное заблуждение.

В настоящее время огромные объемы информации передаются, хранятся, выбираются и обрабатываются миллионами пользователей. Имеется большое количество информационных угроз. В простейшей модели с двумя абонентами, которые посылают друг другу конфиденциальную информацию по единственному каналу связи, рассматривается простейшая угроза чтения этих данных пассивным противником. Классический результат Шеннона [3] показывает, что в этом случае конфиденциальная передача данных возможна. Зачастую этот результат пытаются распространить на модели с более широкими классами угроз. Проблема не только в том, что нет научного обоснования. Существуют угрозы, от которых невозможно защититься в принципе. Далее мы рассмотрим некоторые примеры.

1. Облачные вычисления

Недавний прорыв в математической криптографии — а именно, решение долго остававшейся открытой проблемы пол-

ного гомоморфного шифрования (FHE) — привел к возникновению устойчивого заблуждения. Весьма широко распространено мнение, что FHE решает по крайней мере теоретическую проблему защиту информации в облачных вычислениях. На самом деле доказано [5], что безопасные облачные вычисления невозможны уже в случае двух пользователей.

Этот отрицательный результат не исключает возможности защиты информации в облачных вычислениях для некоторых приложений. Но общего решения быть не может. Может даже оказаться так, что всякое новое приложение (или небольшой класс таковых) требует исследования возможности безопасных облачных вычислений.

2. Скрытые каналы

Одной из хорошо известных угроз является применение криптографии преступным сообществом для пересылки информации через общедоступные сети связи. Здравый смысл поддерживает казалось бы очевидное решение, а именно, ограничение прав использования криптографических методов. В этом случае преступное сообщество может переключиться на использование стеганографии.

Бытует мнение, что использование стеганографии может быть предотвращено, если имеются эффективные методы обнаружения скрытых каналов. Однако существуют так называемые подпороговые каналы [4], которые не могут быть обнаружены даже теоретически.

Может оказаться, что «разумное решение», состоящее в ограничении использования криптографии, на самом деле превращает трудно решаемую проблему в нерешаемую.

3. Обфускация

Компьютерные программы представляют собой специфическую разновидность информации. Обычно защита программ рассматривается как битва против компьютерных вирусов. Но класс угроз программному обеспечению шире, он включает, в частности, нарушение прав интеллектуальной собственности.

Большинство проблем, связанных с защитой программ, могут быть решены, если доступна доверенная программно-аппаратная платформа. Однако, как правило, пользователь выполняет свои программы во враждебной среде. Поэтому остается последняя возможность: программа должна защи-

щать сама себя. Исследования, основанные на этой идее, привели к появлению понятия обфускации. Это эквивалентное (т.е. сохраняющее функциональность) преобразование программы, которое делает её трудной для понимания.

Самое сильное определение обфускации требует, чтобы противник, имеющий доступ к тексту обфускированной программы, не мог извлечь из нее больше полезной информации, чем из поведения этой программы на уровне вход–выход. Доказано [2], что такая сильная обфускация невозможна. За этим последовал ряд работ, в которых были доказаны схожие отрицательные результаты для более слабых моделей. Подводя итог, можно сказать, что возможность защиты программ во враждебной окружающей среде остается открытой проблемой.

4. Сетевая безопасность

Рассмотрим математическую модель большой сети связи и простейшую угрозу недоставления сообщения адресату. Предполагается, что абоненты сети могут быть одного из следующих типов. Сотрудничающие абоненты всегда следуют коммуникационному протоколу. Эгоистичные абоненты не демонстрируют никакого злонамеренного поведения, но, с другой стороны, могут не желать расходовать ресурсы и в некоторых случаях отказываются передавать сообщения. Злонамеренные абоненты никак не ограничены в своем поведении.

Такая модель сети связи анализировалась с использованием теоретико-игровых методов. Равновесия по Нэшу соответствующих игр показали (см. [1]), что сценарии с эгоистичными и злонамеренными абонентами более оптимистичны, чем с сотрудничающими и злонамеренными.

На первый взгляд это может показаться парадоксом. На самом деле, такое мнение основывается на распространенном убеждении, что наилучшим решением для обеспечения информационной безопасности является создание централизованной службы. Однако эта точка зрения никак не обоснована.

Математические результаты поддерживают следующую гипотезу: хаотическая природа больших сетей оказывается лучшей защитой от злонамеренного поведения абонентов.

5. Законы о киберпреступлениях

В связи с законами о киберпреступлениях идет интенсивное обсуждение, как эти законы должны работать, и никако-

го внимания не уделяется основному вопросу: что суд может признать доказательством киберпреступления.

Рассмотрим простой пример математической модели электронных водяных знаков (в литературе используется неадекватный термин «цифровые водяные знаки»). Правообладатель интеллектуальной собственности, существующей в электронной форме, желает доказать арбитру, что данный файл содержит встроенный им (правообладателем) электронный водяной знак. С этой целью он предоставляет арбитру некоторую конфиденциальную информацию, размер которой измеряется мегабайтами. Затем на этих данных выполняется сложная программа, которая работает много часов и в итоге выдает copyright правообладателя. Что в этой ситуации должен делать арбитр?

Приемлемое доказательство может выглядеть примерно так. Правообладатель показывает арбитру картинку и говорит: «Замените все синие и желтые пиксели на белые, все красные и зеленые на черные, и тогда в правом верхнем углу вы увидите мою собственноручную подпись».

Заметим, что мы рассмотрели идеализированную модель, где для всего имеются строгие математические определения. Но проблема арбитража не решена. Что же говорить о «доказательствах» киберпреступления в реальной жизни.

6. Заключение

Общее направление исследований в области информационной безопасности выглядит следующим образом:

- для данных множеств приложений и угроз определить математическую модель;
- в этой модели исследовать существование решений для задач обеспечения информационной безопасности;
- в случае положительного ответа разработать соответствующие методы и системы.

Заметим, что по сравнению с простейшим случаем конфиденциальной передачи данных в общем случае ситуация меняется радикально. Нет надежды на общее решение или на стандарты. В наихудшем возможном сценарии для каждого нового приложения потребуется новый цикл исследований и разработок.

Отрицательные результаты доказываются в математических моделях. Это означает, что даже в идеальном случае решений нет. В реальных сценариях никакие «умные решения» невозможны из-за основной угрозы.

Литература

[1] Tansu Alpcan and Tamer Başar. *Network Security: A Decision and Game Theoretic Approach*. Cambridge University Press, 2011.

[2] Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil Vadhan, and Ke Yang. On the (im)possibility of obfuscating programs. *J. ACM*, 59(2):6:1–6:48, May 2012.

[3] Claude E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal, Vol 28, pp. 656–715*, October 1949.

[4] Gustavus J. Simmons. Subliminal communication is easy using the DSA. In Tor Helleseth, editor, *EUROCRYPT'93*, volume 765 of *Lecture Notes in Computer Science*, pages 218–232. Springer, 1993.

[5] Marten van Dijk and Ari Juels. On the impossibility of cryptography alone for privacy-preserving cloud computing. In *Proceedings of the 5th USENIX Conference on Hot Topics in Security*, HotSec'10, pages 1–8, Berkeley, CA, USA, 2010. USENIX Association.

N.P.Varnovskiy, O.A.Logachev, V.V.Yashchenko
Lomonosov Moscow State University Institute of Information Security Issues

Mathematics and Information Security

Was man nicht weiß, das eben brauchte man
Und was man weiß, kann man nicht brauchen
— Johann Wolfgang von Göthe. "Faust"

Information security is an extremely attractive topic. Search engines when feeded with this term return hundreds millions of references to resources in V^6 ($= W^3 =$ WWW). However when term "information security" is combined with "mathematics" the figures are orders of magnitude lower. This in part reflects common belief that information security is a management task, not a scientific problem. Therefore the role of mathematics is restricted to provide methods, such as data encryption, raw materials for constructing security systems.

This is a great misunderstanding.

Currently huge amounts of information are transmitted, stored, retrieved and processed by millions of users. Threats to information are numerous. In the simplest model of two abonents who sent confident data over an only channel one considers the simplest threat of reading this data by passive adversary. The classical result due to Shannon [3] says that in this setting secure data transmission is possible. One is tempted to extrapolate this possibility result to models with wider classes of threats. The problem is not only in the lack of justification. For certain threats there is no solution. Next we consider some examples.

1. Cloud computing

Recent breakthrough in mathematical cryptography, namely solution of the long-standing problem of fully homomorphic encryption (FHE) caused a lot of misunderstanding. It is widely believed that FHE solves, at least theoretically, a problem of secure cloud computing. In fact, it is proved [5] that secure cloud computing is impossible already in the case of two users.

This negative result does not rule out a possibility of secure cloud computation in certain applications. But there is no general solution. It could even be the case that any new application (or a

small class thereof) requires investigation of possibility of secure cloud computing in this given setting.

2. Covert channels

One of the well-known threats is that of employing cryptography by criminals for sending information over networks. The common sense suggests an evident solution, namely, restricting the right of using cryptographic methods. In this circumstances criminals might resort to steganography.

It is believed that steganography usage can be suppressed if one has efficient methods for detecting covert channels. However there exist so-called subliminal channels (see [4]) which could not be detected even theoretically.

It might be the case that the "clever solution" of restricting usage of cryptography turns a hard to solve problem into a unsolvable one.

3. Obfuscation

Computer programs constitute a specific brand of information. It is common to consider program security as a battle against computer viruses. But the class of threats to software is larger, it includes, e.g., violations of intellectual property.

Most of the problems of program security could be solved if a trusted platform is available. However, as a rule users run their programs in adversarial environment. Therefore there remains ultimate chance. A program should secure itself. Research stimulated by this informal idea resulted in the concept of obfuscation. This is an equivalent (i.e. preserving functionality) transformation of a program that renders the latter unintelligible.

The strongest definition of obfuscation requires that adversary given an obfuscated program can extract no more useful information than that given by input-output behavior of the same program. Such a strong obfuscation was shown [2] to be impossible. This was followed by a number of papers proving related negative results in somewhat weaker settings. Stated in short, the possibility of protecting programs in adversarial environments remains questionable.

4. Network security

Consider a mathematical model of a large scale communication network and the simplest threat of failing to deliver messages to

addressees. Abonents of the network are assumed to be of one of the next types. Cooperative abonents always follow communication protocol. Selfish ones do not exhibit adversarial behaviour but on the other hand they do not want to spend much resources and sometimes refuse to transmit messages. Malicious abonents are not restricted in their adversarial behaviour.

Such a model of communication network was analysed using game-theoretic methods. Nash equilibria of corresponding games show (see [1]) that scenarios with selfish and malicious abonents are more optimistic as compared with the case of cooperative and malicious ones.

At the first glance this might seem to be a paradox. In fact, this point of view is based on the common belief that the best thing to do for providing information security is to establish a centralized hierarchical service. But there is no justification for this opinion.

Mathematical results suggest the next hypothesis: chaotic nature of large scale networks turns out to be the best defence against malicious behaviour of abonents.

5. Law enforcement

In the context of cybercrime law there is an extensive discussion of how this should work. And no attention is paid to the main question: what can be taken by a court as an evidence of cybercrime.

Consider a simple example of a mathematical model for electronic watermarks (in literature a misleading term "digital watermarks" is used). An owner of intellectual property that exists in electronic form wants to prove to arbiter that a file in question has e-watermark embedded by him (the owner). To this end he exposes to arbiter some private information that might be a multi-megabyte string. Then a complicated program runs on these data for hours and finally outputs owner's copyright. What should an arbiter do in such a case?

An acceptable proof might look like this. An owner shows to arbiter a picture and says: replace all blue and yellow pixels by white, red and green by black ones and then in the right upper corner you would find my hand-written signature.

Note that we consider an idealized model where everything has rigorous mathematical definitions. But the problem of arbitration is not solved. Nothing to say about real-life "evidence" of cybercrime.

6. Conclusion

The general line of research in the field of information security is as follows:

- for given sets of applications and threats define a mathematical model;
- in this model study existence of solution to the information security problems;
- in the case of positive answer devise appropriate methods and systems.

Note that in the general case situation changes drastically as compared to the case of secure data transmission. There is no hope for general solutions or standards. In the worst possible scenario each new application would require a complete R&D cycle.

Negative results are proved in mathematical models. This means that solutions do not exist even in idealized settings. In real-life scenarios no "clever solutions" are possible due to the main threat.

References

[1] Tansu Alpcan and Tamer Başar. *Network Security: A Decision and Game Theoretic Approach*. Cambridge University Press, 2011.

[2] Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil Vadhan, and Ke Yang. On the (im)possibility of obfuscating programs. *J. ACM*, 59(2):6:1–6:48, May 2012.

[3] Claude E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal, Vol. 28, pp. 656–715*, October 1949.

[4] Gustavus J. Simmons. Subliminal communication is easy using the DSA. In Tor Helleseth, editor, *EUROCRYPT'93*, volume 765 of *Lecture Notes in Computer Science*, pages 218–232. Springer, 1993.

[5] Marten van Dijk and Ari Juels. On the impossibility of cryptography alone for privacy-preserving cloud computing. In *Proceedings of the 5th USENIX Conference on Hot Topics in Security*, HotSec'10, pages 1–8, Berkeley, CA, USA, 2010. USENIX Association.

E**ighth International Forum** «Partnership of State Authorities, Civil Society and the Business Community in Ensuring International Information Security» and Ninth Scientific Conference of the International Information Security Research Consortium April 21–24, 2014. Garmisch-Partenkirchen, Munich, Germany, 2014. — Moscow: Moscow University Press, 2014. — 288 p.

The proceedings of the Eighth International Forum «Partnership of State Authorities, Civil Society and the Business Community in Ensuring International Information Security» and the Ninth 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

Восьмой международный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» и Девятая научная конференция Международного исследовательского консорциума информационной безопасности 21–24 апреля 2014 года

Текст публикуется в авторской редакции
с оригинал-макета, представленного заказчиком

Подписано в печать 17.10.2014. Формат $60\times90^{1}/_{16}$.
Бумага офсетная. Офсетная печать.
Гарнитура Ньютон. Усл. печ. л. 18,0.
Уч.-изд. л. 14,93.
Тираж 200 экз. Изд. № 10 274. 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

Отпечатано в типографии МГУ.
119991, ГСП-1, Москва, Ленинские горы, д. 1, стр. 15