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

and

Seventh Scientific Conference of the International Information Security Research Consortium

April 22–25, 2013
Garmisch-Partenkirchen, Munich, Germany

Moscow. 2013

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

и

Седьмая научная конференция Международного исследовательского консорциума информационной безопасности

22-25 апреля 2013 года
г.Гармиш-Партенкирхен, Германия

Москва. 2013 г

СОДЕРЖАНИЕ

В.А.Садовничий
Академик Российской Академии наук
Ректор Московского государственного
университета имени М.В.Ломоносова

КАК ЗАЩИТИТЬ ЧЕЛОВЕКА ОТ ИНФОГЕННЫХ РИСКОВ И УГРОЗ?

Массовое освоение киберпространства: позитивные и негативные тенденции

Одной из устойчивых тенденций современного экономического и социального развития является постоянное возрастание роли глобальных информационно-коммуникационных технологий и сетей, особенно сети Интернет. Глобальная информационная сеть объединяет сегодня огромное количество людей – около двух миллиардов человек, предоставляя всем недоступные прежде возможности для общения и сотрудничества (это почти треть населения планеты). Интернет стал неотъемлемой частью общества и экономики, залогом экономического роста и социального развития. Он стал одной из основных движущих сил глобальной экономики, фактором стимулирования роста и инновационного развития. Разнообразные предметно-ориентированные информационные сервисы и услуги – эффективный функциональный элемент практически всех сфер жизни общества: производства, управления, образования, науки, культуры и других. Они придают новое измерение развитию цивилизации, что выражается в концепциях постиндустриального информационного общества и экономики, основанной на знаниях.

Вместе с тем созданная за последние десятилетия разветвленная система информационных инфраструктур (или, другими словами, киберпространство) предоставляет новые возможности для реализации все более изощренных угроз личности, обществу и государству, приобретающих комплексный, транснациональный характер. Не проходит и дня без сообщений о разного рода кибератаках, кибермошенничествах, киберпреступлениях и даже о грядущих (или реальных?) кибервойнах. Источниками таких угроз могут быть и отдельные личности, и организованные группы преступной или террористической направленности, а в некоторых случаях и государственные структуры. Ежегодный ущерб только от компьютерной преступности уже оценивается триллионами.

При этом следует особо подчеркнуть единство проблематики глобальной информационной безопасности, заключающееся в том, что хакеры, кибермошенники, «хактивисты», виртуальные террористы и комбатанты действуют в едином информационном пространстве, используют методы и средства, которые близки по своему назначению, многие из них построены по идентичным техническим принципам, нацелены на одни и те же объекты критических инфраструктур, используют одни и те же их уязвимости.

В последнее десятилетие глобальное информационное пространство всё больше превращается в арену межгосударственного соперничества, борьбы за достижение стратегических и тактических политических целей. В 2011 году опубликованы стратегии кибербезопасности ряда крупнейших держав мира (США, Великобритания, ФРГ и др.), в которых провозглашается курс этих стран на строительство кибервооруженных сил. Американские военные доктринально закрепили за киберпространством статус пятого театра военных действий (наряду с сушей, водой, воздухом и космосом).

Приведенные факты подтверждают вывод, сделанный в докладе Генерального секретаря ООН в 2010 году: «Существующие и потенциальные угрозы в сфере информационной безопасности относятся к числу наиболее серьёзных проблем XXI века».

Принятие норм безопасной деятельности в киберпространстве – императив нашего времени

Поэтому сегодня самый главный вызов всей нашей киберкорпорации – научному сообществу, информационному и сетевому бизнесу и профильным государственным структурам – состоит в следующем: «Как сохранить весь позитивный потенциал киберпространства и вместе с тем нейтрализовать негативные и деструктивные тенденции его использования?».

На мой взгляд, одним из первоочередных шагов на пути к созданию атмосферы доверия в киберпространстве должна быть разработка и принятие на уровне Организации Объединенных Наций документа, закрепляющего фундаментальные принципы деятельности в киберпространстве и обеспечения безопасности этой деятельности. К числу таких принципов относятся, в частности, следующие:

1. Киберпространство является общечеловеческим достоянием и имеет огромный позитивный потенциал для обеспечения устойчивого развития цивилизации.

2. Деятельность в киберпространстве должна способствовать общему экономическому и социальному развитию, включая возможность свободного доступа к ресурсам в киберпространстве в равной степени для всех. Эта деятельность должна быть ограничена только такими формами и действиями, которые соответствуют согласованным общепризнанным принципам и нормам глобальной кибербезопасности.

3. Национальные усилия по защите критических киберинфраструтур должны гармонично сочетаться с широким международным сотрудничеством в области формирования и реализации фундаментальных принципов деятельности в киберпространстве и обеспечения безопасности этой деятельности.

4. Принципы и нормы глобальной кибербезопасности должны быть совместимы с задачами поддержания международного мира и безопасности, соответствовать общепризнанным принципам и нормам международного права, включая принципы мирного урегулирования споров и конфликтов, неприменения силы, невмешательства во внутренние дела, уважения прав и основных свобод человека.

5. Принципы и нормы глобальной кибербезопасности должны быть совместимы с правом каждого искать, получать и распространять информацию и идеи, как это зафиксировано в соответствующих документах Организации Объединенных Наций, с учетом того, что такое право может быть ограничено законодательством в целях защиты интересов национальной и общественной безопасности каждого государства, а также предотвращения неправомерного использования и несанкционированного вмешательства в информационные ресурсы.

6. Доверие и безопасность в использовании информационно-коммуникационных технологий относятся к главным опорам информационного общества, поэтому необходимо поощрять, формировать, развивать и активно внедрять устойчивую глобальную культуру кибербезопасности.

7. Массовое безопасное освоение киберпространства должно опираться на соответствующие научно-технические прорывы и реализацию масштабных образовательных проектов в этой области.

8. Информационный и сетевой бизнес должен быть социально-ответственным и руководствоваться фундаментальными принципами деятельности в киберпространстве и обеспечения безопасности этой деятельности.

Проблемы формирования системы международной информационной безопасности

Все мировое сообщество признает наличие и актуальность проблем информационной безопасности, что отражается в серии ежегодных резолюций Генеральной Ассамблеи Организации Объединенных Наций «Достижения в сфере информатизации и коммуникаций в контексте международной безопасности» (1999-2010) и серии резолюций по вопросам создания глобальной культуры кибербезопасности (2007-2009).

Проблематика информационной безопасности находится в фокусе внимания политического руководства ведущих мировых держав. На саммите «Группы восьми» во Франции в 2011 году лидеры государств обсуждали эти вопросы в числе основных, что отражено в Довильской декларации. В рамках «Группы восьми» создана специальная постоянно действующая подгруппа по вопросам борьбы с преступлениями в сфере высоких технологий – Римско-Лионская группа.

В мировом сообществе де-факто началось формирование региональных систем международной информационной безопасности. Первым шагом в данном направлении стало подписание в июне 2009 года в России в г. Екатеринбурге Соглашения между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области международной информационной безопасности. Организация Договора о коллективной безопасности также наметила направления сотрудничества между государственными органами государств-членов Организации в деле противодействия преступлениям в сфере компьютерной информации и компьютерного терроризма. Активно развивается региональная система обеспечения безопасности информационного пространства государств-членов НАТО от враждебного использования информационных и коммуникационных технологий.

Формируются механизмы практического взаимодействия между государствами, не входящими в региональные системы международной информационной безопасности или принадлежащим к различным региональным системам.

Вместе с тем, как показали события 2011 года, до принятия общепризнанных правил поведения, мер доверия и, уж тем более, юридически обязывающих норм, ещё далеко. Исключительно важно отметить, что среди причин такого положения дел есть и не до конца решенные научные проблемы технического, юридического, философского характера, которые по существу и составляют такую область, как «научное обеспечение переговорного процесса».

Пока не удалось сблизить понятийный аппарат, используемый в разных странах, что существенно затрудняет разговор на международных встречах и консультациях. Нет единой трактовки даже таких базовых понятий, как «информационное пространство» и «киберпространство», «информационная безопасность» и «кибербезопасность».

Не разработаны эффективные алгоритмы определения (а тем более доказательства) источника кибератак в глобальной сети. Поэтому в известных случаях международных резонансных киберинцидентов виновные доподлинно не известны, они просто назначаются из политических соображений с помощью шумных пропагандистских кампаний.

Не разработаны математические модели и индикаторы, позволяющие выделять на фоне огромного количества разнонаправленных, внешне хаотических кибератак признаки скоординированного кибернападения на критически важные объекты. Такие модели и индикаторы предназначены для того, чтобы уже на ранних этапах включать военно-политические и дипломатические механизмы деэскалации киберконфликтов и предупреждения кибервойн.

Не проведен сравнительный анализ различных воззрений на целесообразность и возможность введения в международно-правовой оборот таких концепций, как «Интернет-границы государства», «сетевой суверенитет», «вмешательство во внутреннее информационное пространство другого государства».

Не удаётся разработать эффективные международно-правовые механизмы расследования киберпреступлений, различные этапы которых совершаются в различных юрисдикциях. А между тем количество таких трансграничных преступлений, в которых задействована масса посредников, компьютеров-прокси и бот-сетей, постоянно растёт.

Нет научно обоснованных механизмов мотивации социальной ответственности информационного и сетевого бизнеса.

Мало философских, культурологических и психологических исследований в области киберэтики, которые должны обосновать рекомендации по формированию глобальной культуры информационной безопасности. А ведь если уменьшить количество массовых нарушений элементарных правил поведения пользователей в киберпространстве, можно предотвратить многие киберпреступления.

Долг научно-образовательной корпорации – разработать и внедрить систему знаний, навыков и норм глобальной культуры информационной безопасности

Ликвидация безграмотности в области информационной безопасности – настолько острая и глобальная задача, что её решение не под силу только специализированным государственным структурам. Необходимо объединение усилий науки, образования, средств массовой информации, бизнес-структур, сообществ Интернет-пользователей. При этом первая скрипка здесь за наукой и образованием, которые должны дать инструментарий для решения поставленных задач – научно-обоснованные рекомендации, широкий спектр специальных образовательных программ, методик преподавания, учебной и научно-популярной литературы.

Viktor A. Sadovnichy
Member of the Russian Academy of Sciences,
Rector of Lomonosov Moscow State University

PROTECTING PEOPLE FROM INFORMATION RISKS AND THREATS

Positive and negative trends of large-scale cyberspace development

An increasingly growing importance of global information and communication technologies and networks, especially the Internet, presents one of the persistent trends of modern economic and social development. Today, the global information network brings together as many as two billion people worldwide (which is almost a third of the world's population), offering us unprecedented capabilities to communicate and cooperate. The Internet has become an essential part of society and economy, securing economic growth and social development. It is now one of the main drivers of global economy, an incentive of growth and innovation. A wide range of application-oriented information services offer an effective functional element in almost every domain of life, including manufacturing, governance, education, science, culture, etc. These services take our civilization to a new dimension of evolution through the concepts of post-industrial information society and knowledge-based economy.

At the same time, a manifold system of information infrastructures (in other words, cyberspace) that has been established in the course of the past decades, gives rise to new sophisticated threats to personal, social and national interests, and these threats are gradually becoming multidimensional and transnational. Every single day, we hear reports of various cyber attacks, cases of computer fraud, cyber crime and even upcoming (or already fairly real?) cyber wars. Sources of such threats may be represented by individuals, organized criminal or terrorist groups, and in some cases even government institutions. Annual damages caused by computer crime alone are already estimated in trillions.

Special emphasis should be placed on the uniformity of global information security agenda, which implies that hackers, cyber fraudsters, "hacktivists," virtual terrorists and combatants operate in a single information space and use such tools and resources that are cognate in their intended purpose, largely have an identical design philosophy, are targeted against the same critical infrastructure assets and designed to hit common weak points in such assets.

In the course of the past decade, global information space has become more of an arena for state-on-state antagonism and struggle for strategic and tactical political goals. A number of world powers, including the USA, Great Britain, Germany, etc., published their cyber security strategies in 2011, proclaiming their commitment to build cyber forces. The US Department of Defense officially announced cyberspace as the fifth theater of operations (along with the land, air, sea and space).

The above facts bore out the conclusion made by the UN Secretary General in his 2010 report: "Existing and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century."

Recognizing the standards of secure cyberspace operations is imperative in the modern world

This is why the most serious challenge for our entire cyber corporation, which includes the scientific community, information and electronic businesses, and specialized governmental structures, is how to preserve the best opportunities offered by cyberspace and neutralize the adverse and destructive trends of its application.

In my opinion, one of the first priority steps to building an atmosphere of trust in cyberspace is the development and adoption by the United Nations of a document that would set forth the fundamental principles of activity in cyberspace and guarantee security of such activity. These principles are as follows:

1. Cyberspace is a common heritage of the mankind that has a tremendous potential for sustainable development of our civilization.

2. Activity in cyberspace should promote overall economic and social development and offer equal opportunities for free access to resources in cyberspace. This activity should be limited only to such formats and actions that meet the generally recognized and approved principles and standards of global cybersecurity.

3. National efforts focused on protecting critical cyberspace infrastructures should fall in line with broader international cooperation in the field of designing and deploying fundamental principles of activity in cyberspace and securing cyberspace activity.

4. The principles and standards of global cybersecurity should be consistent with the objectives of global peace and security and meet the generally recognized principles and standards of international law, including peaceful settlement of disputes and conflicts, non-use of force, non-interference in the internal affairs, and respect of basic human rights and freedoms.

5. The principles and standards of global cybersecurity should be consistent with the right of everyone to search, receive and distribute information and ideas, as stipulated by corresponding United Nations documents, in recognition of the fact that such right may be restricted by law as a way to protect the interests of national and public security of each state and to prevent unauthorized tempering with information resources.

6. Trust and security in the use of information and communication technologies make the foundation of the information society, which is why we must encourage, model, develop and aggressively deploy sustainable global cyberspace culture.

7. Large-scale secure development of cyberspace should rely on appropriate breakthrough achievements in science and technology and deployment of ambitious educational projects in this sphere.

8. Information and electronic business must adhere to social commitments and be motivated by the fundamental principles of activity in cyberspace and securing such activity.

Challenges of building the international information security system

All members of the international community recognize the existence and significance of information security issues, which is manifested in a series of annual resolutions of the United Nations General Assembly known as " Achievements in the Sphere of Information Tasks and Telecommunications in the Context of International Security" (1999-2010) and a number of resolutions on global cybersecurity culture matters (2007-2009).

Information security issues are in the focus of attention of political leaders of major world powers. During the G8 Summit in France in 2011, leaders of the states discusses these issues among other critical matters, which is reflected in the Deauville declaration. A special permanent sub-group for high-tech crime matters was established within the G8, officially known as the Roma-Lyon Group.

De-facto, the international community started building regional systems of international information security. The first step in this context was the agreement among the governments of SCO member-states on cooperation in the field of international information security signed in Yekaterinburg (Russia) in June 2009. Collective Security Treaty Organization also has set the lines of cooperation among CSTO members in the field of combating cyber crime and cyber terrorism. Another rapidly growing system is the regional system for securing the information space of NATO member-states from hostile use of information and communication technologies.

Countries that are not members of any regional systems of international information security or those participating in certain regional systems, are also developing approaches for practical cooperation.

At the same time, events of 2011 showed that we still have a long way to go before we adopt any universally recognized rules of conduct and confidence-building measures, not to mention legally binding norms. It is significant that this situation is caused, among other things, by the fact that there are still some outstanding technical, legal and philosophic issues that essentially constitute the domain of "scientific background for the negotiation process."

There is no harmony in the conceptual framework used in different countries, which significantly obstructs understanding at international meetings and consultations. The parties to negotiations do not have a unified interpretation even for such fundamental notions as "information space" and "cyberspace," "information security" and "cybersecurity".

There are no effective procedures to identify (let alone confirm) sources of cyber attacks on the global network. This is why the actual culprits of noted international high-profile cyber incidents remain behind the scenes and are in fact named through political appointment in the course of bustling propaganda campaigns.

There are no mathematical models or indicators in place that would help distinguish the signs of coordinated cyber attacks on critical facilities among the ocean of multidirectional and seemingly chaotic cyber attacks. Such models and indicators would allow engaging the military-political and diplomatic arrangements for de-escalation of cyber conflicts and prevention of cyber wars at early stages.

There has been no benchmarking of different views on practicability and feasibility of introducing into the international legal language of concepts like "Internet boundaries of the state," "network sovereignty," or "intervention into the information space of a foreign nation."

The efforts aimed at developing effective international legal mechanisms for investigation of cybercrimes whose different stages are committed in different jurisdictions have been unsuccessful. Meanwhile, the number of such criminal cross-border activities involving numerous intermediaries, proxy computers and botnets is continuously increasing.

There are no scientifically proven mechanisms for inducement of social responsibility of the information and network businesses.

The number of philosophic, cultural and psychological surveys in cyber ethics that are supposed to validate the recommendations for the development of global

information security culture is fairly small. At the same time, if we could reduce the number of wide-scale violations of basic rules of conduct in cyberspace, many instances of cyber crime would have been prevented.

The goal of the research and educational corporation is to design and deploy a system of knowledge, skills and standards of the global information security culture

Fight against illiteracy in the information security domain is a serious global challenge that cannot be addressed only by special government agencies. It requires uniting the efforts of scientific and educational communities, mass media, private businesses and communities of Internet users. The leading role will be assigned to the scientific and educational communities that are expected to provide a toolkit for handling the problems that exist, such as scientifically founded recommendations, a wide range of special educational programs, teaching techniques, study materials and popular scientific literature.

ヴィクトル・A・サドーヴニチィ

ロシア科学アカデミーの正会員

M.V.ロモノーソフ・モスクワ国立総合大学学長

どうしたら情報的なリスクと脅威から個人を守れる？

サイバースペースの大規模な開発：正負のトレンド

現代の経済及び社会開発における、一貫したトレンドの一つとしては、グローバル的な情報通信技術及び、ネットワーク、特にインターネットの役割が継続的に増加している。グローバルな情報ネットワークで世界人口の1／3に等しい大多数の人々（約20億人）がつながっている。そのネットワークを介して、以前利用不能であったコミュニケーション及びコラボレーションができるようになった。インターネットは社会や経済の不可欠な部分、又は経済成長と社会の発展の鍵となっている。世界経済の主要な原動力の一つで、成長と革新的開発を促進する要因となった。多様なサブジェクト（主題）指向の情報サービスやアメニティは、生産及び、管理、教育、科学、文化などの、社会におけるほぼ全ての生活圏に係わる効果的な機能要素であり、脱工業化の情報化社会と知識型経済の概念で表現され、文明の発展に新たな次元を与える。

ただし、過去数十年間で編み出された大規模な情報インフラのシステム（いわゆるサイバースペース）を利用して、個人及び社会、国家への手口の巧妙化な脅威は、高度化と国際化が進んでいる。ほぼ毎日サイバー攻撃やサイバー詐欺などを含む、多様なサイバー犯罪類、さらに将来的及び現在のサイバー戦争についてのニュースが届いている。これらの脅威の発生源は、個人も、犯罪やテロ組織にも関連し、いくつかのケースでは、或る政府機関がある。コンピュータ犯罪行為からの年次損失は推定が数兆ルーブル相当であると評価される。

しかも、グローバルな情報セキュリティ上、共通する問題点があることを強調すべきである。ハッカー、サイバー詐欺師、ハクティビスト、仮想テロリスト及び戦闘員などは、共通の情報空間にて行動し、目的で類似している方法および手段を使用している。それらの多くは、同一技術的な原理に基づいて開発され、同様な脆弱性を使用し、同じ洋な重要なインフラをターゲットにしている。

過去10年間で、グローバルな情報空間はますます国家間競争、戦略的および戦術的な政治目的達成用の闘争の舞台になりつつある。2011年に数国の大国（米国、英国、ドイツなど）はサイバーセキュリティ戦略が公表され、その国はそれぞれがサイバー軍を設立するように宣言した。米軍の戦闘教義で、サイバー空間は、陸、海、空、宇宙に続き「第5の戦闘領域」と認識されるようになってきている。

この事実は、2010年の国際連合事務総長の「情報セキュリティの分野で、既存および潜在的な脅威は、二十一世紀の最も深刻な課題の一つである」という報告書の結論を確認する。

サイバースペースでの安全活動規則の採択は、我々の時代の急務である。

従って、現在、科学者コミュニティ、情報通信やネットワークビジネスおよび国家機関に関連する我々にとって、最も重要な直面する挑戦は、次の点である：「どうやってサイバースペースのすべての将来性を維持すると同時に、その使用よって生じるネガティブおよび破壊的な効果を中和するか？」。

私の意見では、サイバースペースにおける信頼の雰囲気の創出に向けた最優先のステップの一つが、国連によってサイバースペースでの基本的な活動原則および、セキュリティを確立する、公的な書類を開発し、採用すべきである。このような原則は、とくに次に示す：

1. サイバースペースは、人類の共通の遺産であり、文明の持続可能な開発のための大きな将来性を秘めている。
2. サイバースペースにおける活動は、すべてに等しくサイバースペース内のリソースへの自由なアクセスを含めて、全体的な経済･社会の発展に貢献すべきである。この活動に制限をかける際、共通に合意されたグローバルサイバーセキュリティ原則や規範に従ってする。
3. 国の取り組みで重要なサイバーインフラを保護される際、サイバースペースにおける基本的な活動原則および安全確保活動の、開発と実施の分野における広範な国際協力と組み合わせる必要がある。
4. グローバルサイバーセキュリティの原則と規範は、国際の平和及び安全の維持と互換性がある必要があり、紛争や対立の平和的調和、力の不使用、内政不干渉の原則を含む、一般に公正妥当と認められた国際法の原則や規範を遵守し、人権及び基本的自由の尊重を維持する。
5. グローバルサイバーセキュリティの原則と規範は、情報及び考えを求め、受け及び伝える自由を含む、国連の適切な書類によって記録されてある原則に遵守しなければならない。しかし、国家安全保障、公共の安全および、情報リソースの誤用又は不正な干渉の防止のために法律によって制限される場合は有り得る。
6. 情報通信技術の利用の信頼性とセキュリティは、情報化社会の主要な柱である。従って、積極的に持続可能なグローバルなサイバーセキュリティ文化を奨励・促進・開発・実装されるべきである。
7. サイバースペースの集団的に安全な開発は、関連する科学技術のブレークスルーと、この分野における大規模な教育プロジェクトの実施に基づくべきである。
8. 情報通信およびネットワークビジネスは社会的責任を持って、サイバースペースにおける基本的な活動原則によって導かれ、この活動の安全を確保すべきである。

国際情報セキュリティシステムの形成の問題点

全世界の国際社会は、情報セキュリティ上の課題の有無との関連性を認識している。国連総会第一委員会による「国際安全保障の文脈における情報及び電気通信分野の進歩」の年次決議（1999-2010年度）および、世界的なサイバーセキュリティ文化の開発に関する総会の決議（2007-2009年度）のシリーズにて反映されている。

情報セキュリティの課題は、世界有数の大国の政治指導者の焦点にある。2011年にフランスにて開催された「G8」首脳会議で、国家の指導者は、重要な課題間でこれらの課題を議論したこと、ドーヴィル宣言文に反映されている。「G8」グループ下、ハイテク犯罪と闘うための特別恒久サブグループを設立し、「ローマ・リヨングループ」と名称さらた。

国際社会は、国際的情報セキュリティの地域システムの形成されている。この方向での最初のステップは、ロシアのエカテリンブルク市で、2009年6月に国際的な情報セキュリティの分野における協力に関する、上海協力機構の政府間の協定が成立になったことである。集団安全保障条約機構も同じ方向に向かい、加盟国の当局間、コンピュータ情報およびコンピュータテロの分野における犯罪との協力分野を特定している。NATO加盟国は、情報通信技術の敵対的使用に対する情報空間地域セキュリティシステムを積極的に開発している。

国際情報セキュリティ地域システムに属されてない国および、異なる地域システムに属している国間の交流方法などは、新たに実質的な協力メカニズムとして開発されている。

しかし、2011年のイベントで、一般的に受入可能な行為規則と信頼醸成措置、さらに、法的拘束力のルールなどの採用が程遠いことが示された。現在のその状況に至った原因の一つとしては、一般的に「交渉プロセスにおける科学的支援」と思われる、技術、法律、哲学、科学的な問題が完全に解決されてないことを強調すべきである。

それぞれの国（特にロシア、米国）で使用される概念的枠組みが、未だ調整することができてないため、国際会議や協議において話し合いが困難であるため、「情報空間」、「サイバースペース」、「情報セキュリティ」及び「サイバーセキュリティ」などの基本的な概念でも、単一の解釈がない。

インターネット上のサイバー攻撃の発信元（さらに、その証拠）を決定するため効率的なアルゴリズムが開発されてない。したがって、知られている国際的にインパクトのあったサイバーインシデントの加害者が不明であり、政治的な理由で単にうるさいプロパガンダキャンペーンによって加害者が任命される。

異なる方向の膨大な数のあるサイバー攻撃の中、一見混沌とした重要施設に対するサイバー攻撃から協調した攻撃であるの兆しを読み取る数学的モデル及び、目立つ指標はない。そのモデルや指標は、初期の段階で軍事や政治的及び、外交的なメカニズムを用いてサイバー紛争のエスカレーションとサイバー戦争の防止の意図している。

「インターネット上の国境」、「ネットワーク主権」及び「他国の内部情報空間への干渉」などの概念の国際法的導入の必要性や可能性に関する異なる見解の比較分析ができてない。

様々な法域にて犯罪ステージが発生するサイバー犯罪に対する、国際法的で効果的な取り調べ方する法を開発ことは、なかなかできていない。一方、仲介や代理コンピュータ及びボットネットの多くが関与させる、複数の国境を越える犯罪の数は増え続けている。

社会的責任をもった情報通信ネットワーク事業のエビデンスベースのモチベーションのメカニズムがない。

世界的な情報セキュリティの文化を創るための勧告などを論証し、サイバー倫理の分野における哲学的、文化的、および心理学的研究の結果が不足している。しかし、サイバースペースにてのユーザーの行動における基本ルールの大規模違反の数を減らすだけで、多くのサイバー犯罪を防ぐことができる。

教育機関は世界的な情報セキュリティの文化の知識、スキルや基準の仕組みを開発し、実装する義務がある。

情報セキュリティに関する非識字状態を改善するのは、急性的でグローバルな課題であるため、専門の政府機関にて解決策を開発し実施するしかないと思われる。科学、教育、メディア、企業、インターネットユーザーのコミュニティの総合的な協力が必要である。ただし、リーダーシップは科学と教育業界にあるべきである。エビデンスに基づいた勧告、特殊な教育プログラムや指導方法、教育と科学専門の大衆教材など、直面する課題を解決するために必要になる、広い範囲のツールを編み出される必要があるためだ。

如何消除信息产生的危险与威胁

人类如何消除来自信息领域的危险与威胁

维克多·安东诺维奇·萨多夫尼奇

俄罗斯科学院院士

罗蒙诺索夫莫斯科国立大学校长

大规模网络发展：利与弊

全球信息通讯技术与网络、尤其是互联网的发展，是当代经济与社会稳定发展的主要趋势之一。目前国际互联网的使用者人数已近20亿，为人们的交流与合作提供了空前的机会。互联网已成为社会与经济发展不可或缺的一部分，也是经济成长与社会发展的重要保障，同时还是促进全球经济成长的动力与创新发展的因素。不同信息服务几乎涵盖了所有社会生活领域，诸如生产、管理、教育、科学、文化等等。后工业时代的信息社会及以知识为基础的新经济观念，显示文明的发展有了新的变化。

近几十年信息设施系统所建立的众多分支，也就是网络空间，反而给目前更为严重的威胁提供新的机会，而这些威胁对个人、社会与国家，是全面性的与跨国性的。我们每天都会受到各种有关的网络攻击、网络诈骗、网络犯罪，甚至可能在未来发生现实的网络战争。因此，个人、罪犯或恐怖组织、有时是国家机构都会成为该威胁的来源，同时每年因网络犯罪造成的损失估计已经达到数万亿。

特别强调的是全球信息安全的问题应该是一致的，也就是黑客、网络诈骗、计算机激进分子、网络恐怖分子或战士在网络空间活动所使用的具体方法和手段中都有近似的方式，不少是源于相同的技术原理与基础，也都是针对重要的基础设施。

为达到战略和战术的目的，近十年来，国际信息空间已逐渐成为国际竞争或争斗的场所。2011年一些世界主要国家如美国、英国，德国等，先后公布了其网络安全战略，宣布组建网军，美国的军事学说更把网络空间定为第五战场（跟陆、海、空和天并列）。

上述事实有力的支持了2010年联合国秘书长在其报告中所得出的结论——
信息安全领域所面临的现有的和潜在的威胁可以说是二十一世纪最严重的安全问题。

遵守网络空间活动安全的准则在当前是绝对必要的

因此，我们的网络社团——科学团体、信息与网络工业和相关的国家机构——
目前最主要的挑战是，如何发展运用网络空间之“利”并抵制消除其“弊”。

在我个人看来，要形成网络空间里互相信任的氛围，首要步骤是拟定经联合国审定的文件以规范网络空间活动的基本原则。这些原则包括：

1. 网络空间是人类的共同财产，对人类文明的稳定发展具有巨大的促进作用。

2. 网络空间的活动应该是正面的，能促进经济和社会发展的。所有人对网络空间的资源都应享有同等的使用自由，并受某些规范的约束和限制。人们在网络空间的活动应该符合国际网络安全公认的原则与准则。

3. 国家应该努力通过广泛与和谐的国际合作来保护重要网络设施，这些合作应着重于落实网络空间活动的基本原则与保证网络空间活动的安全。

4. 全球网络安全的原则和准则应与维持国际和平与安全的任务相一致，并符合国际法公认的原则和准则，包括：以和平方式解决争论与争端、不诉诸武力、不干涉内政、尊敬个人权利与基本自由等原则。

5. 全球网络安全的原则和准则应遵照联合国有关文件的规定，出于各国保护国家和社会安全的考虑，以及防止信息资源的违法使用，个人搜寻、接收与传播信息的权利需受到法律的约束。

6. 信息通信技术的安全是信息社会的重要支柱，因此需要促进网络安全文化的形成和发展，并加以全球性的积极推广。

7. 应该以科技手段及普及教育促进公众开发安全的网络空间。

8. 信息与网络交易应该对社会负责，遵守网络空间活动原则并保证网络空间活动的安全。

建立国际信息安全体系的问题

一系列联合国年度大会的决议如《国际安全形势下信息化与通信方面的成果》(1999-2010)与建立全球网络安全文化的系列决议(2007-2009)表明，国际社会已认识到信息安全问题的紧迫性。

世界主要国家的政治领导人对信息安全的问题表达了高度的重视。2011年在法国举行的八国峰会上，各国领袖在主要议题上讨论了这些问题，形成了《多维尔宣言》，并在八国集团的管辖范围内专门设立常设的小组来防范高科技犯罪，即罗姆里昂小组。

事实上，国际社会针对国际信息安全已开始形成区域性的体系。在这方面，2009年六月在俄罗斯叶卡捷琳堡市上海合作组织成员国政府之间签署了有关国际信息安全合作的协议，迈出了可贵的第一步。集体安全条约组织也以相同方式，在对抗计算机信息犯罪和网络恐怖行动的领域里拟定该组织成员国国家机关之间的合作方向。北约成员国的地区体系对于防范敌人使用信息和通信技术的攻击获得了积极发展，维护着网络空间安全。

未参加国际信息安全区域体系且属于不同区域体系的国家之间的实际交流机构也正在形成之中。

与此同时，2011年的事件表明，如何建立公认的准则与互信措施、甚至有法律约束力的规范，其实还有很长的路要走。特别是造成这种情况的原因在于技术、法律、哲学等仍有未完全攻克的难关，这些具体问题造成在谈判过程中科学领域难以做出有力的保证。

各国之间关于网络概念至今还无法取得一致认可，尤其是在俄罗斯和美国之间，这在很大程度上妨碍了在国际场合和国际会议上的交流与沟通，而一些基本概念也没有共通的解释，比如：信息空间和网络空间、信息安全和网络安全。

至今我们仍然没能找到网络攻击的规律，因此在重大的国际网络事件中犯罪情况难以追责，政治家往往以臆想的政治理由来制造轰动一时的新闻宣传。

至今还没有建立能够在纷繁复杂的诸多信息中指认出针对最重要设施的网络攻击的数学模型和指示器。在未来，这样的模型和指示器可以被运用于早期预警，并进而启动网络冲突降级与网络战争预防的军政和外交工具。

关于国家互联网边境、网络主权、干涉异国信息空间等概念进入国际法的可能性与适当性分析讨论还没有进行。

现在还没有创立出认定网络罪行的有效国际法机制，而且更复杂的是，网络罪行的不同阶段在不同司法权范围内进行。同时，许多中间人、代理计算机和机器人参与的跨界网络犯罪也越来越多。

但是，目前尚没有使信息和网络交易对社会负责的科学根据。

在控制论方面的哲学、文化学和心理学的研究相当少，而这些研究应该对国际信息安全文化的形成提供助力。不过，如果减少用户在网络空间的违规行为，可以预防许多网络罪行。

科学教育团体的责任在于推广国际信息安全文化、技能与准则

专门的国家机构无法应付全面积极推广信息安全知识的任务，应该整合科学、教育、媒体、商业机构和网络用户社团的力量，同时科学和教育团体应该担负起领导的作用，提出行动纲要，也就是科学地规划各种专门的教育纲要，推广教学与学习的方法，编撰科普书籍。

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

АКТУАЛЬНЫЕ ПРОБЛЕМЫ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Уважаемые участники Форума и гости! Дамы и господа!

Рад приветствовать Вас в Германии, в г.Гармиш-Патенкирхен на очередном, Седьмом заседании нашего Форума, посвященном обсуждению важнейших проблем обеспечения международной информационной безопасности на основе партнерства государства, бизнеса и гражданского общества.

Германия не случайно стала местом наших ежегодных встреч. С одной стороны, это одно из центрально-европейских государств, член Европейского союза, который активно занимается проблематикой противодействия угрозам кибербезопасности как важной составной части деятельности по обеспечению национальной безопасности. С другой стороны, в силу своего географического положения Германия является прекрасным местом, где могут собираться эксперты различных политических взглядов и свободно обмениваться мнениями по трудным проблемам формирования системы международной информационной безопасности. Это создает хорошие условия для уяснения позиций международных экспертов по вопросам, выносимым на обсуждение участников Форума, и поиску путей сближения этих позиций.

Благодаря этому за прошедшие годы существенно расширился состав участников Форума, а также представительство на нем специалистов различных государств мира.

В этом году в работе Форума принимает участие более 100 ученых и специалистов из 18 государств мира. К числу таких государств относятся Австрия, Азербайджан, Бахрейн, Беларусь, Великобритания, Германия, Индия, Италия, Казахстан, Канада, Китай, Куба, Россия, США, Франция, Швейцария, Эстония и Япония.

В работе конференции принимают участие представители Организации по безопасности и сотрудничеству в Европе и Международной корпорации по присвоению доменных имен и адресов.

Для участия в Форуме в Германию прибыла большая группа специалистов и ученых из России. Среди них представители аппарата Совета Безопасности Российской Федерации, МИДа России и Минобороны России, представители ведущих компаний, входящих в состав российской Ассоциации защиты информации, а также большая делегация Московского государственного университета.

Делегацию аппарата Совета Безопасности Российской Федерации, осуществляющего подготовку предложений Президенту Российской Федерации по вопросам информационной безопасности, возглавляет Беляев Иван Иванович, который является сопредседателем Оргкомитета Форума.

Вам известно, что усилиями всех заинтересованных участников Форума в 2010 г. был образован Международный исследовательский консорциум информационной безопасности. В его состав на сегодня входят 17 организаций и ассоциаций. Это Институт проблем информационной безопасности МГУ имени М.В.Ломоносова, Объединенный институт проблем информатики Национальной Академии наук Беларуси, Интернет-сообщество Болгарии, Институт исследований вопросов киберпреступности (Германия), Департамент информационной безопасности электронного правительства Израиля, Индийский институт информационных технологий в Аллахабаде, Китайское общество дружбы с зарубежными странами, Телекоммуникационная компания «МФИ Софт» (Россия), Университет штата Нью-Йорк, Компания «Глобал Сайбер Риск» (США), Университет Токай (Япония), Институт «Восток-Запад» (США), Организация оборонных исследований и разработок Министерства обороны Индии, Хазарский Университет (Азербайджан), Компания PayPal Inc. (США), Университет «Кавказ» (Азербайджан), а также неправительственная организация The

SecDev Foundation, занимающаяся исследованиями вопросов глобальной безопасности и развития (Канада).

Несмотря на небольшое время, прошедшее с момента образования Консорциума, усилиями экспертов, входящих в его состав, удалось выполнить ряд совместных проектов и, в частности, силами специалистов ИПИБ МГУ и Института Восток-Запад разработать базовые положения понятийного аппарата (глоссария) по тематике информационной безопасности, предназначенные для поддержки переговорного процесса по формированию системы международной информационной безопасности. Первый этап этого проекта завершился изданием брошюры на русском и английском языках, содержащей подробные комментарии к 20 базовым терминам в области кибербезопасности. Брошюра размещена в сети Интернет и уже активно цитируется в публикациях по тематике международной информационной безопасности. В настоящее время идет работа по второму этапу данного проекта, который должен закончиться к концу 2013 года изданием аналогичной брошюры с трактовкой очередных 20 базовых терминов в области информационной безопасности. Близок к завершению второй проект, в котором принимают участие все члены Консорциума, посвященный анализу национальных законодательств по вопросам фильтрации Интернет-контента.

Участники Форума – ИПИБ МГУ и Исследовательский центр по изучению конфликтов (Conflict Studies Research Centre) (Великобритания) – в 2012 году реализовали совместный проект по анализу положений концепции Конвенции об обеспечении международной информационной безопасности. Результаты работы размещены в сети Интернет.

Таким образом, Форум де-факто стал одной из важных площадок обсуждения различных аспектов тематики международной информационной безопасности.

Мы весьма признательны тем участникам Форума, которые смогли поддержать Форум не только личным участием, но и существенными финансовыми средствами. Среди них хотелось бы отметить генерального директора ФГУП НТЦ «Атлас» Гридина Александра Николаевича, генерального директора компании «РНТ» Новикова Андрея Алексеевича, первого заместителя генерального директора – научного руководителя НИИАС (РЖД) Матюхина Владимира Георгиевича, вице-президента международной корпорации ICANN Вени Марковски, заместителя генерального директора Координационного центра национального домена сети «Интернет» Романова Андрея Георгиевича.

Большое всем спасибо за то, что вы откликнулись на приглашение организаторов и прибыли сюда для участия в работе Форума.

Актуальность тематики нынешнего Форума обусловлена, с одной стороны, тем, что все большее количество государств начинает понимать необходимость координации усилий международного сообщества в противодействии угрозам снижения доверия граждан, бизнес-организаций, органов государственной власти к использованию информационных и коммуникационных технологий. Эти технологии обладают огромным потенциалом повышения эффективности социально-экономического развития общества, укрепления государственных гарантий реализации прав и свобод человека и гражданина, усилий государственных органов по поддержанию обороноспособности страны и безопасности государства. Снижение доверия к информационным и коммуникационным технологиям было бы значительным ударом по надеждам международного сообщества на дальнейшее повышение качества жизни людей, расширение их возможностей самореализации, снижение уровня бедности и повышение доступности качественного образования.

Многолетние совместные усилия различных государств мира, международных организаций, организаций бизнеса и экспертного сообщества по изучению проблематики международной информационной безопасности и принятию практических мер по повышению безопасности функционирования информационных систем и коммуникационных сетей принесли свои плоды. Сформировалось общее понимание того, что наиболее опасными угрозами международной информационной безопасности на данном этапе являются продолжающийся рост масштабов компьютерной преступности, подготовка и осуществление актов компьютерного терроризма, а также использование информационных и коммуникационных технологий для «силового» разрешения межгосударственных противоречий.

Вопросы, вынесенные на обсуждение участников Форума, так или иначе связаны с формированием системы международной информационной безопасности, которая призвана способствовать развитию глобального информационного общества, использованию информационных и коммуникационных технологий на благо человека и общества.

Всех нас объединяет понимание того, что для развития глобального информационного общества необходимо обеспечить эффективное противодействие угрозам устойчивому функционированию и безопасному использованию глобальной информационной инфраструктуры, основу которой составляет Интернет. Жизненно важно противодействовать

угрозам превращения Интернета в театр военных действий или идеологических сражений и при этом обеспечить информационную безопасность каждого государства мира.

На круглом столе нашего Форума предусмотрено обсуждение вопросов, связанных с сохранением Интернета как пространства свободы, а также основных тенденций в области его использования для оказания давления на противостоящие государства. Представляется, что поиск путей сохранения позитивного потенциала влияния глобальной информационной инфраструктуры на развитие человечества – задача чрезвычайно важная и заслуживает самого пристального внимания со стороны участников дискуссии. Мы надеемся, что в ходе дискуссий удастся определить границу, за которой свобода обмена мнениями между людьми в Интернете превращается в действия государств, которые можно рассматривать как вмешательство во внутренние дела других стран. Возможно, нам удастся понять пути решения данной проблемы.

Другим важным вопросом, вынесенным на рассмотрение Форума, является поиск путей практической интернационализации управления Интернетом. Превращение Интернета в общедоступный глобальный инструмент ставит управление его использованием одним из ключевых элементов формирования глобального информационного общества. Представляется, что интернационализация управления использованием Интернета будет содействовать поддержанию высокого уровня доверия к этому уникальному средству межчеловеческого взаимодействия, участию в этом процессе заинтересованных правительств, представителей частного сектора, гражданского общества и международных организаций. Интернационализация должна способствовать справедливому доступу к ресурсам Интернет, облегчать доступ для всех и обеспечивать стабильное и безопасное функционирование Интернета. Мы рассчитываем на то, что в результате работы круглого стола будет достигнут достаточно высокий уровень взаимопонимания, необходимый для разработки практических механизмов интернационализации управления Интернетом на основе баланса интересов и полномочий государственных органов, организаций бизнеса и гражданского общества.

На одном из круглых столов Форума предлагается обсудить подходы различных государств к решению проблем обеспечения безопасности национальной инфраструктуры, лучшие национальные практики. Актуальность данного вопроса во многом определяется тем, что для достижения конкретных практических результатов в области обеспечения национальной

информационной безопасности необходимо вовлекать в этот процесс значительные группы граждан, организации гражданского общества, заинтересованные политические и экономические силы. Только совместными усилиями можно добиться равноправного и безопасного доступа всех государств мира к информационным и коммуникационным технологиям.

Другим важным вопросом повестки дня Форума является проблема организации фильтрации Интернет-контента. Актуальность данной проблемы обусловлена, в первую очередь, потребностью общества в нейтрализации негативных последствий злоупотребления свободой информации во вред общественной нравственности, социальной стабильности и здоровью подрастающего поколения. Ряд специалистов рассматривает данное явление как одну из форм цензуры. С формальной точки зрения это, наверное, правильно. Но реальная практика современной жизни такова, что в той или иной степени механизмы фильтрации Интернет-контента используются многими государствами мира, в том числе и теми, которые относят себя к весьма демократическим. Представляется, что нас не должны пугать названия. Важно найти те правовые и организационные механизмы укрепления международного сотрудничества, которые помогут сохранению общественной нравственности, социальной стабильности и здоровья детей.

Одной из важнейших проблем современного этапа формирования национальных систем обеспечения информационной или кибербезопасности, а также проблем обеспечения международной информационной безопасности является налаживание взаимовыгодного сотрудничества в этой области между организациями бизнеса и органами государственной власти, отвечающими за национальную безопасность. Многие объекты экономической деятельности давно стали критически важными объектами национальной информационной инфраструктуры. Обеспечить безопасность данных объектов без взаимодействия организаций бизнеса и государственных органов не представляется возможным. В то же время найти эффективные механизмы такого взаимодействия пока не удается. Надеюсь, что обсуждение на Форуме поможет в поиске конструктивного ответа и на этот вопрос.

Трудно переоценить значение механизмов международного правового регулирования для обеспечения международной информационной безопасности. Право является мощным средством координации и упорядочения усилий всех государств мира в противодействии угрозам компьютерной преступности, компьютерного терроризма и агрессивного использования информационных и коммуникационных технологий. Один из круглых сто-

лов нашего Форума будет посвящен обсуждению проблем международного правового регулирования отношений, возникающих в связи с информационными конфликтами. Как известно, совсем недавно международному экспертному сообществу было представлено «Таллиннское руководство о применимости международного права к киберконфликтам». Было бы правильно и на нашем Форуме начать обсуждение этого документа и направлений дальнейшей работы в данной области. К числу таких направлений в первую очередь относится разработка рекомендаций по адаптации международного права к регулированию информационных конфликтов.

Новым и очень важным научным направлением в области противодействия агрессивному использованию информационных и коммуникационных технологий является моделирование информационных конфликтов. На Форуме обсуждению возникающих в этой области проблем и способов их решения предполагается посвятить отдельный круглый стол.

В заключение позвольте выразить надежду, что совместными усилиями нам удастся продвинуться на пути укрепления плодотворного международного сотрудничества в интересах реализации потенциала информационных технологий для улучшения жизни человека, обеспечения устойчивости общественного развития.

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

INTERNATIONAL INFORMATION SECURITY: ACTUAL CHALLENGES

Dear Participants and Guests of the Forum! Ladies and Gentlemen!

I am pleased to welcome you all at the Forum's seventh meeting held in Garmisch-Partenkirchen, Germany. The Forum will discuss topical issues of international information security in the format of partnership between the government, business and civil society.

It is no accident that our annual Forum is held here, in Germany. On the one hand, Germany is a Central European power and a member of the European Union which is actively engaged in countering threats to cyber security as an important component of the overall national security. On the other hand, in view of its favorable geographical position, Germany makes a perfect venue for experts representing various political opinions to get together and exchange their views on the difficult problem of forming a solid system of international security. This greatly facilitates understanding between international experts and helps find ways to reconcile their positions towards the discussion items on the Forum's agenda.

Over the recent years the number of the Forum attendees has grown considerably while their geography expanded.

This year the Forum will be attended by more than 100 scientists and experts representing 18 countries, including Austria, Azerbaijan, Bahrain, Belarus, the United Kingdom, Germany, India, Italy, Kazakhstan, Canada, China, Cuba, Russia, the USA, France, Switzerland, Estonia and Japan.

Representatives of the Organization for Security and Cooperation in Europe (OSCE) and the International Corporation for Assigned Names and Numbers (ICANN) will also attend the Forum.

A numerous group of Russian experts and scientists have arrived to Germany to take part in the Forum. The group includes representatives of the Executive Office of the Russian Federation Security Council, the Russian Federation Ministry of Foreign

Affairs and the Russian Federation Ministry of Defense as well as representatives of leading companies who are members of the Russian Information Protection, and a large delegation from the Moscow State University.

The delegation of the Executive Office of the Russian Federation Security Council, whose function is to advise the Russian Federation President on the issues relating to information security, is headed by Ivan I. Belyaev, a co-chair of the Forum's Organizing Committee.

As you are well aware, in 2010 the Forum stakeholders put their efforts together to found the International Information Security Research Consortium. Today the Consortium includes 17 organizations and associations: the Information Security Institute at Lomonosov Moscow State University, the United Institute of Informatics Problems of the National Academy of Sciences of Belarus, The Internet Community of Bulgaria, the Cybercrime Research Institute (Germany), the Israeli E-government Information Security Department, Indian Institute of Information Technology in Allahabad, the Chinese People's Association for Friendship with Foreign Countries, a telecommunications company "MFI Soft" (Russia), the State University of New York, Global Cyber Risk (USA), Tokai University (Japan), EastWest Institute (USA), the Defence Research and Development Organisation of the Indian Defence Ministry, Qafqaz University (Azerbaijan), PayPal Inc. (USA), University of the "Caucasus" (Azerbaijan), non-governmental SecDev Foundation engaged in global security and development research (Canada).

Despite the short time since the formation of the Consortium, its experts have already implemented a number of joint projects, in particular, the experts from the Information Security Institute at Lomonosov Moscow State University (ISI LMS) and EastWest Institute have developed the basic terminology (the glossary) in the area of information security to support the negotiating process with the view to establish the international information security system. As the result of Phase I of the above project a brochure containing detailed commentary to 20 basic cybersecurity terms was published in Russian and English. The brochure is available on the Internet and is actively referred to in other publications on international information security. The project is currently in Phase II which will be completed by the end of 2013 with another publication detailing other 20 basic terms in information security. Another project involving the study of provisions in national legislations with regard to Internet content filtering which have brought together the efforts of all the members of the Consortium is also nearing completion.

In 2012 the ISI LMS and the Conflict Studies Research Centre (the UK), both the Forum participants, implemented a joint project related to the study of the

provisions of the Convention on International Information Security. The results of this project are available on-line.

Thus the Forum has de facto become one of the most important platforms to discuss various discuss various aspects of international information security.

Please allow me to express our deep gratitude to the Forum attendees who support the Forum not only with their personal participation but also with substantial funding. Here I would like to name of few names: Alexander N. Gridin, director general of FSUE STC "ATLAS", Andrei A. Novikov, director general of "RNT", Vladimir G. Matyukhin, first deputy director general and research manager of NIIAS (Russian Railways), Veni Markovski, vice president of ICANN, Andrei G Romanov, deputy director general of the Internet National Domain Coordination Center.

I would like to convey to all of you the gratitude of the Organizing Committee for accepting our invitation and attending the Forum.

The significance of this year's agenda of the Forum is very high as ever more nations begin to realize the urgent need for coordination of the international effort to curb the growing mistrust of information and communication technologies among citizens, business organizations, and public authorities. Such technologies have an enormous potential in improving the socio-economic development of the human society, reinforcing state guarantees of human and civil rights and freedoms, and facilitating national defense and state security. Further decline in confidence in information and communication technologies would be hard blow to the expectations of the international community of enhancing people's quality of life and self-realization, reducing poverty and providing better access to high-quality education.

The joint effort of many years of a number of nations, international organizations, business organizations and the expert community relating to the study of the problem of international information security and implementation of practical measures to enhance security of information systems and communication networks has finally paid off. A common understanding of the most dangerous threats to international security of the present day has been reached. Such threats include the growing cybercrime activity, preparation and implementation of acts of cyberterrorism, and the use of information and communication technologies in hostilities between nations.

All the items on the Forum's agenda are one way or another related to the formation of the system of international information security which aims to promote the development of the global information society and the use of

information and communication technologies for the benefit of individuals and the human society as a whole.

We all understand that formation of the global information society requires efficient means to counter threats to stable operation and safe use of the global information infrastructure which is based on the Internet. It is of vital importance to combat the threats of turning the Internet into a theater of war or ideological hostilities while preserving information security of each nation.

The agenda of the round-table discussion at the Forum includes the issues related to the preservation of the Internet as "the space of freedom", as well as the discussion of major trends in the use of the Internet as a means of exerting pressure onto the nations in conflict. We understand that maintaining the positive impact of the global information infrastructure onto the mankind development is an issue of extreme importance and deserves a close attention from the panelists. We hope by way of our discussions to identify the borderline beyond which the freedom of exchange of ideas between people on the Internet becomes an act of the state which must be regarded as interference in the internal affairs of other nations. Perhaps we can find ways of solving this problem.

Finding ways to internationalize control over the Internet is another important item on the Forum's agenda. Development of the Internet as a publicly available global tool makes the control of its use one of the key elements of the now forming global information society. It appears that internationalization of control mechanisms over the use of the Internet will help maintain a high level of confidence in this unique tool of interpersonal communication, facilitate participation of national governments, the private sector, the civil society, and international organizations. Internationalization must promote fair access to Internet resources, provide easier Internet access for everybody and ensure stable and secure operation of the Internet. We expect to reach a high level of understanding between the round-table participants that would facilitate the development of efficient mechanisms to internationalize the control over the Internet while preserving the balance of interests and powers of national authorities, the business and the civil society.

One of the Forum's round-tables will be devoted to the discussion of a range of approaches and best national practices exercised by different nations to ensure security of the national infrastructure. The relevance of this issue is largely determined by the fact that achievement of practical results in building national information security requires involvement of a large masses of populace, civil organizations, political and economic forces. Only by a joint effort we can hope to achieve fair and secure access to information and communication technologies for all the nations of the world.

The problem of filtering Internet content is another very important issue on the Forum's agenda. The urgency of this problem is dictated by the urge to neutralize negative effects of abuse of freedom of information to the detriment of public morality, social stability and health of the younger generation. Some experts may consider such practices to be a form of censorship, which is probably correct from a formal perspective. At the same time the reality of the present day is such that many nations apply varying degrees of Internet content filtering, even the nations who otherwise consider themselves to be very democratic. We are of an opinion that formal definitions should not prevent us from the search for proper legal and organizational mechanisms to reinforce international cooperation to preserve public morality, social stability and health of our children.

One of the major problems of the present moment in forming national systems of information and cyber security and ensuring international information security is to establish mutually beneficial cooperation in this area between business organizations and the public authorities responsible for national security. Many economic assets have now become critically important elements of the national information infrastructure. Ensuring security of such assets without efficient interaction between business organizations and public authorities is not deemed possible. At the same time, really efficient mechanisms of such interaction yet remain to be found. We can hope that constructive discussions at the Forum will help us find an answer to this question.

It is hard to overestimate the importance of the mechanisms of international legal regulation in ensuring international information security. Law is a powerful means of coordinating and streamlining the efforts of all world nations in countering the threats of computer crime, computer terrorism and abuse of information and communication technologies. One of the round-tables at the Forum will be devoted to the discussion of the problem of international legal regulation of relations arising from information-related conflicts. As you well know, The Tallinn Guidelines on Applicability of International Law to Cyberconflicts was quite recently submitted to the expert community. It would be a right thing to do to commence discussions of the above document at our Forum and any further work required to be done in the area. An example of the latter may be the development of recommendations regarding adaptation of international law to regulating information conflicts.

Modeling of information conflicts is an emerging very important area of research in counteracting hostile use of information and communication technologies. This problem and possible solutions will be discussed at the Forum at a separate round-table.

In conclusion I would like to express my hope that together we can move forward in promoting further fruitful international cooperation in realizing the true potential of information technology to improve the lives of people and securing sustainable social development.

И.И.Беляев
Сопредседатель оргкомитета Форума,
референт Аппарата Совета Безопасности
Российской Федерации

О ПОДХОДАХ К КОНСОЛИДАЦИИ УСИЛИЙ МИРОВОГО СООБЩЕСТВА ПО ПРОТИВОДЕЙСТВИЮ УГРОЗАМ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Уважаемые участники конференции! Уважаемые коллеги! Позвольте от имени руководства аппарата Совета Безопасности Российской Федерации и от себя лично приветствовать организаторов, участников и гостей международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности».

В седьмой раз гостеприимный Гармиш-Партенкирхен собрал представителей органов власти, ученых и экспертов научных и образовательных центров ведущих мировых держав. Участники форума встретились вновь, чтобы обсудить наиболее острые проблемы в области безопасности информационной сферы. Предстоящая встреча очень своевременна, а вопросы, вынесенные на обсуждения, чрезвычайно важны и актуальны.

Очевидно, что активное внедрение информационных и коммуникационных технологий в различные области жизнедеятельности государств ставит в число приоритетных задачу обеспечения международной информационной безопасности.

Мировое сообщество естественным образом переходит к формированию политической, правовой и организационной основы противодействия вызовам и угрозам безопасности в информационной сфере.

Их трансграничный характер повышает уязвимость национальных информационных инфраструктур. Особенно это касается критически важных

для национальной безопасности объектов. Все более частыми стали деструктивные информационные воздействия, представляющие серьезную опасность суверенитету и территориальной целостности любому государству. Кроме того, они могут иметь негативные последствия и для отдельной личности, и для общества в целом.

Сегодня все мы со всей серьезностью осознаем уровень и масштаб новых вызовов и угроз в стремительно развивающейся сфере информационных и коммуникационных технологий. Прогнозируя тяжесть возможных последствий их противоправного использования, мировое сообщество признает объективную необходимость консолидации усилий на данном направлении. Полагаем, что наступает время для формирования нового облика системы международной информационной безопасности. Такой системы, которая была бы устойчива к нарастающей угрозе безопасности глобального информационного пространства.

Определение основных элементов этой системы, условий ее надежного функционирования и эволюции должно стать, прежде всего, темой научных дискуссий и экспертных заключений. Начало этому процессу положила международная встреча высоких представителей, курирующих вопросы безопасности, в сентябре 2011 года в Екатеринбурге. На ней был представлен российский проект концепции Конвенции об обеспечении международной информационной безопасности.

Эта концепция и проблематика в целом уже обсуждались на научном семинаре в рамках прошлогоднего форума в Гармиш-Партенкирхене. В последующем концептуальные подходы обеспечения международной информационной безопасности рассматривались и на других международных площадках, в том числе на конференциях в Чанше, Гонконге, Будапеште и других.

Состоявшиеся дискуссии показали, что идея консолидации усилий мирового сообщества в обеспечении международной информационной безопасности в целом нашла свое понимание. Сегодня потребность в объединении возможностей мировых держав становится все более очевидной. В данном случае даже обладание достаточным ресурсным потенциалом не может гарантировать государству его абсолютную защищенность.

Отмечая ведущую роль государственных институтов в обеспечении информационной безопасности, хотелось бы подчеркнуть, что в данной сфере существует широкий спектр для совместной деятельности государственных структур, институтов гражданского общества, научного, экспертного и бизнес-сообщества. Только на условиях государственно-частного партнерства,

как представляется, можно добиться необходимого результата.

Сегодня на форуме мы вправе говорить о потребности в более активном использовании в этом процессе научно-исследовательского потенциала. Применение на практике накопленных знаний и опыта ученых различных стран позволит определить рациональные меры и механизмы противодействия современным вызовам и угрозам в информационной сфере. Как представляется, объектами исследований в этой области могут стать как сами вызовы и угрозы, так и их источники. Также подлежат всестороннему изучению возможные последствия деструктивного информационного воздействия на национальные, прежде всего критические, инфраструктуры. По нашему мнению, научный подход и системный анализ будут способствовать выработке более действенных мер по противодействию недружественному и противоправному применению информационных и коммуникационных технологий.

Принципиально значимой становится разработка согласованного во всех отношениях понятийного аппарата в рассматриваемой области. Это важное направление приложения сил научного и экспертного сообщества. Как говорил великий Даламбер: «… договоритесь о понятиях и вы снимете половину заблуждений у человечества…». Другая составляющая – возможность совместных научных исследований в области международной информационной безопасности, а также обмен опытом и достижениями, или, как принято говорить сегодня, – лучшими практиками.

Эти и другие меры могут стать первым шагом на пути сближения позиций и единого понимания происходящих процессов в данной сфере. В качестве следующего шага следует рассматривать гармонизацию национальных законодательств в области обеспечения информационной безопасности. Выработанные на унифицированной и согласованной правовой основе меры по обеспечению международной информационной безопасности способны внести весомый вклад мирового сообщества в противодействие нарастающим угрозам.

Уже сегодня основу будущего сотрудничества могут составить единые правила и нормы (кодекс) ответственного поведения государств в информационном пространстве. Необходимость установления таких правил и норм уже признана мировым сообществом. Определенный задел на этом направлении сформирован. Так, в сентябре 2011 года Россия, Китай, Таджикистан и Узбекистан распространили в качестве официального документа 66-й сессии Генеральной Ассамблеи ООН «Правила поведения в области обеспечения международной информационной безопасности». Как представляется, логика со-

бытий требует последовательного продвижения по этому пути.

Полагаю, что тематика вопросов, выносимых на обсуждение, позволит участникам встречи предметно рассмотреть не только обозначенную проблему разработки правил поведения, но и многие другие аспекты обеспечения международной информационной безопасности. Форум дает хорошую возможность обменяться мнениями по наиболее актуальным проблемам, определить направления совместной деятельности по их решению.

Надеюсь, что публичное представление материалов нашего форума станет достойным вкладом в дело консолидации международного сотрудничества и укрепления доверия в глобальном информационном пространстве.

Желаю всем участникам форума успешной и результативной работы.

Dr. Belyaev I.I.,
Co-Chairman of the Forum,
Security Council of the Russian Federation
Information Security Coordinator

ON APPROACHES TO CONSOLIDATION OF INTERNATIONAL EFFORTS TO COUNTER THREATS TO INTERNATIONAL INFORMATION SECURITY

Dear conference participants! My fellow colleagues! Please allow me on behalf of the Executive Office of the Security Council of the Russian Federation and from myself personally to extend the warmest greetings to the organizers, participants and guests of the International Forum Partnership between State, Civil Society and Business in the Field of International Information Security.

This year already for the seventh time Garmisch-Partenkirchen gives a warm welcome to government officials, scientists and experts representing research and educational centers of the world's most developed nations. The Forum participants have got together again to discuss the most pressing issues in the area of information security. The upcoming conference is very well-timed and the problems planned to be discussed are of extreme importance and relevance.

It appears to be quite obvious that any active introduction of information and communication technologies into various areas of operation of the machinery of the state makes international information security one of the top priorities.

As a natural process of further technological development the global community begins to form political, legal and institutional framework to counter challenges and threats to information security.

The trans-border nature of such challenges increases vulnerability of the information infrastructure of a nation. This is especially true for assets with critical importance for the national security. Instances of destructive information activity have now become more frequent and represent a serious threat to sovereignty and territorial integrity of any nation. Furthermore, exposure to such destructive information may have adverse consequences both for individuals and the society as a whole.

Today we are all very aware of how serious and massive the new challenges and threats have become in so rapidly developing a field as information and communication technologies. Well knowing the severity of possible consequences

of abuse of such advanced technologies, the international community recognizes the urgent need to consolidate efforts in this very important area. We truly believe that the time to reconfigure the system of international information security is approaching. The new system must have sound resistance to all new threats to the security of the global cyberspace.

Identifying the essential elements of such system and conditions for its reliable operation and evolution should become, above all, the subject of scientific discussions and expert opinions. The international conference of high-ranking officials responsible for national security held in Yekaterinburg in September 2011 marked the start of the above process. At the conference in Yekaterinburg Russia presented the Draft Concept for the Convention on International Information Security.

The above concept along with its subject problem in general were discussed at a scientific seminar which was a part of the last year's Forum in Garmisch-Partenkirchen. Later on, the conceptual approaches to international information security were also discussed at other international venues, including the conferences in Changsha, Hong Kong, Budapest, etc.

The discussions held so far have shown that the idea of consolidating the efforts of the international community with the purpose of ensuring international information security finds support. Today the need for bringing the potential the world powers together has become ever so evident. Trying to tackle this problem alone even when a nation commands a vast resource potential cannot guarantee absolute security to the state.

It is worthwhile to note the leading role of government agencies in ensuring information security. At the same time, we must emphasize that in this area there is a wide range of opportunities for cooperation between public authorities, institutions of the civil society, the academia, experts in the field and the business community. Only through a partnership between the public and the private sectors the desired results seem practically achievable.

At this Forum we speak of the need for a more active involvement of available research potential. By way of applying the knowledge and experience accumulated by the academia of different nations we could identify efficient measures and mechanisms to deal with the present day challenges and threats in the field of information. It appears that the subject of inquiry may be the challenges and threats themselves or their sources. Also a thorough study of all possible consequences of exposure of critical national infrastructure to destructive information is required. In our opinion, scientific approach and system analysis will facilitate the development

of most efficient measures to counter hostile and unlawful applications of information and communication technologies.

The need for development of a consistent body of terminology in the field in question has lately gained fundamental importance. It is a very important area of application of scientific and research expertise. As the great d'Alembert put it: "... the moment you agree about your terminology you have eliminated a good half of all possible misconceptions..." The other component of great importance would be to organize joint research in international information security and share experience and achievements, or, putting it in the modern language: 'best practices'.

Measures as indicated above and others may prove to be the first step towards reaching a common understanding of the processes currently at play in the area in question. The following step should involve standardization of national legislations with regard to ensuring information security. Provisions for international information security developed under a unified and consistent legal framework shall make a significant contribution of the global community into the program of countering emerging threats.

Even today the foundation for the future cooperation could be laid by introducing uniform rules and regulations (the Code) of responsible behavior of nations in cyberspace. The need for such uniform rules and regulations has been recognized by the international community, and this important work is already underway. In September 2011 Russia, China, Tajikistan and Uzbekistan distributed The International Code of Conduct for Information Security as an official document at the 66th session of the United Nations General Assembly. It appears that the next logical step would be to continue to move down this path.

I believe that the scope of the discussion items will allow the participants to scrutinize not only the above problem of development of applicable rules of conduct, but also many other aspects of international information security. The Forum provides an excellent opportunity to exchange views on the most pressing issues and determine the strategy for the joint effort aimed to address them.

I hope that the publication of the Forum materials will make a considerable contribution into the effort to consolidate international cooperation and reinforce confidence in the global cyberspace.

I wish all the Form participants productive and successful work.

Крутских А.В.
Специальный координатор по вопросам политического использования информационно-коммуникационных технологий, Посол по особым поручениям Министерства иностранных дел России

МЕЖДУНАРОДНЫЙ ПОЛИТИЧЕСКИЙ ПРОЦЕСС ПО НАХОЖДЕНИЮ РЕШЕНИЙ В ОБЛАСТИ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Уважаемые дамы и господа, коллеги!

Прежде всего, хочу выразить признательность оргкомитету нашего форума за приглашение принять в нем участие. В международном политическом лексиконе его уже давно именуют «Давосом по вопросам международной информационной безопасности». Здесь мы имеем хорошую возможность в формальной и неформальной обстановке обсудить эту актуальную и приоритетную проблематику.

Очень сожалею, что основатель и организатор этого форума Шерстюк Владислав Петрович не смог по состоянию здоровья прибыть на него. Благодаря его вкладу и энергии вот уже седьмой год подряд над этим историческим зданием в Гармиш-Партенкирхене целую неделю будет развиваться российский флаг. Надеюсь, что уже в скором времени Владислав Петрович продолжит свою деятельность на благо российской и международной информационной безопасности (МИБ).

Свое выступление я хотел бы посвятить теме, которая еще ни разу не звучала в прямом виде в Гармише – дипломатического или политического «перетягивания каната» в области МИБ. В целях сделать свое выступление максимально объективным, в раскованном аналитическом жанре, оговорюсь, что выступаю не в своем официальном качестве, а, как и большинство здесь сидящих, как эксперт, в своей академической ипостаси.

Выступление будет состоять из эпиграфа, «ужасного» предисловия и, собственно, основной части.

В качестве эпиграфа я хотел бы взять недавние слова пресс-секретаря Президента Российской Федерации (14.04.2013) Д.Пескова, который подчеркнул, что «...вся мировая обстановка диктует необходимость сближения России и Америки». Дело здесь не только в особой ответственности этих стран за глобальную стабильность. Именно с США первыми мы стали обсуждать тему обеспечения МИБ, когда Россия еще в 1998 г. сделала эту проблематику предметом и объектом мировой гласности. К сожалению, сегодня дипломатический и политический «канат» в этой сфере мы по целому ряду ее аспектов держим с разных сторон.

Отмечу, что это отнюдь не значит, что роль других стран не имеет значения. Наоборот, она критически важна. Мы выступаем за участие всего международного сообщества в обсуждении и принятии решений в том, что касается использования информационно-коммуникационных технологий (ИКТ). Есть даже соответствующая формулировка, чудовищно звучащая в русской транскрипции, – «мультистейкхолдеровая модель» участия в переговорном процессе, т.е. правительств, неправительственных кругов, гражданского общества, бизнеса и даже отдельных пользователей. Без гармоничного взаимодействия всех этих акторов трудно выработать режим использования ИКТ, который бы исключал, в силу самой специфики этих технологий, сохранение лазеек (safe heavens) для киберкриминала, кибертеррористов и прочего враждебного применения ИКТ, что сводило бы международное сотрудничество в области обеспечения МИБ на нет.

В силу глобальной природы ИКТ, по моему мнению, какие бы переговоры по МИБ не велись, в т.ч. в региональных форматах, они должны учитывать позицию таких стран как Китай, других членов БРИКС (которая существенно совпадает с российскими подходами), членов ЕС, развивающихся стран. Вырабатываемые региональные и двусторонние меры сотрудничества в области МИБ ни у кого не должны вызывать подозрений и не должны противопоставлять один регион другим.

И еще один момент, объясняющий выбор эпиграфа. Подчас на международных переговорных площадках по МИБ и использованию ИКТ приходится слышать от некоторых ближайших партнеров Вашингтона – договоритесь с США, и за нами дело не станет. Ну что же, будем работать, и, как говорил великий А.А.Громыко, «строить политику с учетом этого фактора».

Теперь «ужасное» предисловие. Сразу оговорюсь, что буду использовать то, что собираюсь сказать, в качестве гиперболы, чтобы лучше выразить свою мысль. Присутствующие в зале журналисты и участники официальных переговоров знают, что я – любитель всякого рода сравнений и аналогий, которые помогают подчас упростить понимание идущих в политической и международной жизни процессов.

Давайте на миг представим, что мы, сидящие здесь, являемся «плохими ребятами» (bad guys), «руководителями наркокартеля» с глобальными амбициями распространить наше зелье по всей планете. Какой системный, на уровне макрорешений подход мы будем реализовывать? Я вижу это следующим образом.

1) Прежде всего, мы постараемся убедить весь мир, что наркотики несут только благо человечеству, что без них жизнь невозможна и, соответственно, нужна полная свобода доступа к ним.

2) Чтобы все могли ими пользоваться, т.е. «подсесть на нашу иглу», надо повсеместно нарастить соответствующий технический и методологический потенциал (capacity building).

3) Чтобы у нас, как говорят, все было и за это нам ничего не было, следует легализовать нашу деятельность, т.е. принять соответствующие внутренние и международные законы. Главное - подменить принцип запрещения нашей незаконной деятельности принципом, что ее жертвы могут в индивидуальном порядке предъявлять претензии нашему глобальному картелю в отдельных случаях.

4) Поскольку у нас есть конкуренты по бизнесу, между ними могут возникать разборки, войны. Чтобы избежать взаимоуничтожения, надо договориться как их вести.

5) В идеале важно гарантировать доходность нашего бизнеса при любом раскладе, а для этого надо обеспечить предоплату наших услуг, т.е. контроль за финансовыми средствами всех потребителей.

Все это стратегическая логика реализации наших преступных планов. Тактика и пропагандистская упаковка наших действий могут быть, естественно, разными.

И, наконец, основная часть моего выступления.

Март был очень насыщенным в плане различных мероприятий в области МИБ – многосторонних и двусторонних переговоров. Хотел бы привлечь ваше внимание к событиям не крупнокалиберным, но весьма

показательным с точки зрения характеристики позиций стран в сфере обеспечения МИБ. В течение марта было сделано два выступления – одно в начале марта мною, другое в конце – моим американским визави из Госдепартамента США Крисом Пейнтером. Мое было на межведомственном совещании, его – на слушаниях в Конгрессе.

Что интересного в этих выступлениях? Не сговариваясь, оба функционера (у нас и должности называются одинаково) – координаторы по вопросам политического использования ИКТ – говорили почти одним профессиональным языком, на одну тему, структурировали доклады практически по одной схеме. Все это указывает на то, что есть общее понимание проблемы и угроз, а также относительно приоритетности темы МИБ, что мы «сидим в одной лодке», и что растет осознание необходимости предпринимать совместные действия, и что в одиночку и даже с ближайшими партнерами вместе никто из нас противостоять негативным последствиям цунами под названием «революция в области ИКТ» не сможет.

Были ли различия? Были! В порядке юмора скажу, что они носили «синтаксический» характер. Там, где мой коллега ставил точку, хотя и выступал вторым, я ставил запятую и делал небольшие дополнения. Конкретизирую это, ибо здесь и заключается суть политического перетягивания каната на многочисленных международных переговорах по дипломатической линии.

Первое. Мы оба с одинаковой степенью страсти, почти в одних и тех же выражениях, обосновывали значимость обеспечения свободы доступа к Интернет и ИКТ в целом. Сама суть этих технологий в их глобальности и общедоступности. С этим никто не спорит. Наверное, можно признать, что свобода пользования ИКТ является одним из основных прав человека. Правда, есть политические «радикалы», которые ставят это право выше всех остальных гуманитарных прав. Такой экстремистский подход трудно разделить, равно как и формальную фиксацию этого права свободы доступа. Свобода без надлежащей ответственности может вести только к анархии, беспределу и порождает угрозу быть использованной во вред самой себе. Не должно быть свободы на доступ у криминала, террористов, агрессоров. Казалось бы, банально и ясно. Но всякий раз, когда мы хотим отразить в международных документах этот баланс свободы и ответственности при использовании ИКТ, начинаются трудности – «канат» политических разногласий натягивается. Про свободу упоминать можно, а про ответственность – нельзя. Происходит подмена понятий: при реализации странами своего суверенитета начинают говорить о цензуре, вмешательстве в дела бизнеса и т.п.

Это «перетягивание каната» вдвойне контрпродуктивно, поскольку проблема сбалансированной трактовки этой темы уже решена человечеством.

В известном Международном пакте «О гражданских и политических правах» от 19 декабря 1966 г. прямо говорится, что пользование такими правами налагает особые обязанности и особую ответственность и может быть, следовательно, сопряжено, с некоторыми ограничениями: а) для уважения прав и репутации других лиц Ь) для охраны государственной безопасности, общественного порядка, здоровья или нравственности населения (ст. 19).

К сожалению, про ответственность в пользовании ИКТ в докладе моего упомянутого коллеги нет ни слова. Точку он ставит сразу после слов о свободе.

Второе. Модной темой в политических дискуссиях на международной арене, связанных с МИБ, в последний год-полтора с подачи США и ряда их партнеров становится тема наращивания потенциала (capacity building). Ее пытаются закрепить в документах «восьмерки», ООН, форумов по борьбе с киберпреступностью, т.е. практически везде, где можно.

Кто же против преодоления «цифрового разрыва» и оказания соответствующего технологического содействия, особенно развивающимся странам?! Одни декларации на этот счет мало что сделают, нужно и уже пора конкретизировать данную программу, снять сомнения, что ее реализация пойдет по назначению, ответить на вопросы, которые мы слышим при двусторонних консультациях с другими странами.

Многие из них высказывают опасения, что такая помощь может превратиться в технологический неоколониализм; стать скрытой формой лоббирования отдельных производителей и закрепления отнюдь не универсальных стандартов технологического развития; обставляться политическими условиями; может негативно сказаться на их суверенитете.

Важно гарантировать, чтобы сама помощь в рамках программы наращивания потенциала, с одной стороны, не стала ширмой для вмешательства во внутренние дела стран-получателей, а с другой – не придала новых сил «цифровому Франкенштейну» и в конечном итоге не нанесла ущерб странам-донорам, и чтобы полученные технологии и навыки (know-how) не использовались в незаконных и злонамеренных (malicious) целях.

Третье. В рамках борьбы с киберпреступностью США и страны Евросоюза активно навязывают миру правовую схему решения проблем уголовного характера, возникающих в сфере использования ИКТ, путем глобализации известной Будапештской конвенции 2001 г. Совета Европы. За 12 лет ее под-

писали 49 государств и ратифицировали 39. Подавляющее большинство государств, включая Россию, воспринимает ее скептически, если не с настороженностью, и присоединяться к ней не собирается.

На наш взгляд, данный документ по существу «дает зеленый свет» вмешательству во внутренние дела других государств и несанкционированному проникновению в их информационное пространство, игнорирует их суверенитет в информационной сфере. К тому же, Конвенция страшно устарела. Как отмечают специалисты, она криминализирует всего 9 видов незаконного использования ИКТ, а сейчас их уже около 30. Она не содержит таких понятий как кибертерроризм, ботнеты, не учитывает реалии правовых систем стран, которые не вошли в привилегированное, но очень ограниченное число ее первоначальных авторов.

Для борьбы с таким глобальным явлением как киберпреступность нужен не «местечковый» подход, а универсальный современный документ, выработанный под эгидой ООН, при открытом для всех стран участии, который бы учитывал все позитивные аспекты Будапештской конвенции и других региональных наработок на этот счет, но также был избавлен от их слабостей и ограничений.

Четвертое. Много шума создается вокруг идеи применимости современного международного права к военно-политическим конфликтам в информационном пространстве или связанным с использованием ИКТ. Здесь очень много неясного, несогласованного, хотя бы уже в силу того, что современное международное право создавалось до революции в области развития и применения ИКТ и, соответственно, без учета порождаемых этим процессом реалий.

На наш взгляд, речь должна вестись не о формально провозглашении принципа применимости, а об адаптации международного права к новым явлениям информационной/цифровой среды. Простой перенос старых норм на новые события может вызвать обратный эффект. Возможно, политикам и юристам надо срочно заняться выработкой новых норм и определений.

Главное понять: мы все за предотвращение кибервойны или за ее регулирование и, следовательно, легитимизацию. Россия однозначно за первый вариант. Второй возрождает пресловутую концепцию 60-х годов разгара вьетнамской войны так называемой «ограниченной ядерной войны» или «ядерной эскалации» вооруженных конфликтов теперь в преломлении к сфере использования ИКТ.

В качестве начала можно было бы подумать о сотрудничестве в области обеспечения информационной безопасности критических инфраструктур и так называемых мер доверия, а не «тянуть канат» по поводу применимости международного права.

Пятое. Экономическая или финансовая сторона МИБ, связанная с национальной безопасностью и социальной стабильностью. Известно, что глобальной и необратимой тенденцией мирового экономического развития является переход финансовых расчетов на виртуальную основу и, соответственно, на практически полное вытеснение наличных денег из обращения.

Возникает далеко не праздный вопрос – не приведет ли в целом позитивных процесс перевода экономики на электронные деньги к новой политической сверхзадаче, реализация которой будет строиться по формуле: кто контролирует использование ИКТ, тот контролирует финансовые потоки и, соответственно, мировую политику? Не станет ли очередное глобальное перераспределение власти внутри олигархических элит, которое обеспечивает господство над мировой экономикой, прологом к катаклизмам, в т.ч. военно-политического характера, в которых «крайним» окажется, как это исторически не раз бывало, человечество?

Как это будет происходить на практике – поясню на конкретном примере. Поскольку вы все устали, сделаю это так, чтобы вызвать улыбку на ваших лицах. Когда в этот раз я приехал в Гармиш, мы с друзьями пошли в соседний магазин, чтобы купить что-то, чтобы отметить сие событие. Из-за технических причин кредитные карточки там не принимались и это что-то нам не продали. Вот вам и социальная нестабильность, чреватая политическими последствиями, особенно если подобные сбои в мировой экономике будут происходить по чьему-то негласному заказу.

В итоге напрашивается простой вывод – «астероид» нашей общей глобальной киберопасности приближается. Времени для принятия политических мер взаимной защиты не прибавляется. Необходимо не тянуть одеяло или канат на себя и уже в обозримой перспективе выйти на конкретные международные договоренности о правилах или принципах ответственного поведения государств, о мерах доверия в информационном пространстве, о предотвращении гонки виртуальных вооружений и киберконфронтации, способных подвергнуть международный мир и безопасность весьма реальному испытанию.

Ambassador Krutskikh A.V.,
Special coordinator
for political use of information and communication technologies,
Ministry of Foreign Affairs, Russia

INTERNATIONAL INFORMATION SECURITY IN INTERNATIONAL POLITICAL PROCESS

Dear Ladies and Gentlemen,

First of all, I would like to express my gratitude to the organizing committee of our forum for the invitation to come here. In international political parlance, it has been known for a long time as 'Davos of International Information Security'. Here, we can have a good opportunity of discussing this hot-spot and top-priority issue in a formal and informal setting.

I am awfully sorry that the founder and the organizer of this forum Vladislav Petrovich Sherstyuk has been unable to get here due to ill health. Thanks to his input and drive, the Russian national flag will be fluttering over this historical building in Garmisch-Partenkirchen during the entire week for the seventh year running. I hope that within a short while, Vladislav Petrovich will continue to benefit the cause of Russian and international information security (IIS).

In my speech, I would like to address the topic that has never before been presented in an explicit manner in Garmisch, that of a diplomatic or political 'tug of war' in the field of IIS. With a view to making my address as fair-minded as possible as and less intense than normally coming from the political pulpit, I am speaking not in my official capacity, like most of you sitting here but as an expert in my academic field.

My speech will include an epigraph, a 'horrible' introduction and, basically, the main part.

As an epigraph, I would like to quote the recent words of Press Secretary of the President of the Russian Federation (14.04.2013) D. Peskov, who stressed that «... the whole world situation calls for closer relations between Russia and America.» This issue has a larger scope than the responsibility of these nations for global stability. The United States was the first nation that we brought up with the issue of policing IIS when Russia made it the subject and the object of the global publicity back in 1998. Unfortunately, today we are facing each other across the opposite sides of the diplomatic and political 'tug of war' on a range of points and views in this area.

Please note that this doesn't imply that the role played by the other nations is immaterial. On the contrary, it is critically important. We encourage the involvement of the entire international community in discussions and decision-making relating to the use of information and communication technologies (ICT). There is even the appropriate term, sounding extremely awkward in the Russian language multi-stake participation model in the negotiation process, i.e. with participation of Governments, non-government bodies, civil society, business, and even individual users. Without well-coordinated interaction of all these actors, it is difficult to develop a way of using ICT that, relying on the specific nature of these technologies, would eliminate the still existing safe heavens for cyber-criminals, cyber-terrorists and other hostile uses of ICT, which would make redundant international cooperation in the field of IIB.

Given the global nature of ICT, I believe that no matter what negotiations are underway on IIS, including at regional level, these should take into account the position of other nations, such as China and the remaining BRICS members (echoing the Russian approach on essential points), members of the EU and developing nations. Regional and bilateral cooperation measures produced in the field of IIS should not make anyone suspicious and should play one region against another.

And there is yet another argument for picking the epigraph. At times I am used to hearing at international meeting venues on IIS and the use of ICT some of Washington's closest partners the message: reach agreement the United States and we will keep our part of the bargain. Well, it will be working, as great Andrei Gromyko once said, «towards building a policy with that thing in mind».

Now we are moving onto the 'horrible' introduction. I will say in advance that I will use what I am going to say as a hyperbole so as to add more clarity to my thoughts. Those journalists and participants in official negotiations attending this meeting know that I am a practiced hand in using all kinds of comparisons and analogies that sometimes help get a more insight into processes ongoing in the political and international area.

Let us for a moment imagine that those who are sitting here, are the 'bad guys', 'drug cartel lords' with global ambitions to extend our 'goods' all over the planet. What systematic macro level decision approach are we going to put into use? I can vision it in the following way.

1) First of all, we will try to convince the world that drugs are only for the benefit of mankind, that life is impossible without them and, therefore, what is needed is completely free access to them.

2) In order to ensure that everyone can use them, i.e. 'get hooked on our needle', it is necessary to build an appropriate technical and methodological capacity.

3) So that, as the saying goes, we would have everything and we wouldn't be liable be for it, our activities should be legalized, i.e. we should adopt appropriate domestic and international laws. The main thing is to substitute the principle of the prohibiting illegal activities for our principle whereby their victims can, on an individual basis, raise complaints with our global cartel in isolated cases.

4) Since we have business rivals, then there can be in-fighting and wars between them. In order to avoid mutual destruction, we must agree on rules of engagement.

5) Ideally, it is important to ensure the profitability of our business in any case and to this end, it is necessary to make a down payment for our services, i.e. to provide control over financial resources of every consumer.

All of these considerations underlie the strategic logic of carrying out our criminal plans. Tactics and ideological wrappings of our activities can, surely, vary.

And, finally, the main part of my speech

March was a hectic time full of various activities in the area of IIS – multilateral and bilateral negotiations. I would like to draw your attention to events that are of no great magnitude, although highly representative of the countries' positions in the field of IIS. During March, two speeches were made, one in the beginning and the other in the end of March, by my American counterpart from the U.S. State Department Chris Painter. My speech was made at an interagency meeting as part of a congressional hearing.

What is interesting about these speeches? Without any collusion, both officials (our respective positions carry the same title) – coordinators on the political use of ICT – were speaking nearly the same professional language, on the same subject and using almost identically structured reports. All this points out to the fact that there is a common understanding of the problem at hand, related threats and the priority status of the IIS issue and that we 'are in the same boat' and there is growing awareness of the need to take joint action, and that none of us, alone or even together with the closest allies, are in a position to confront the adverse tsunami effects dubbed «the ICT revolution».

Were there any differences? Yes, there were! By way of joke, I will say that that they were of syntactic nature. Where my colleague put a full stop, although he was speaking before me, I put a comma and made short additions. The reason

I am specific on this point is it is the essence of a political tug of war in numerous international negotiations through diplomatic channels.

First, both of us were making a case for the significance of Internet access in particular and ICT as whole being in nearly the same passionate way and almost in the same terms. The essence of these technologies lies in their global nature and accessibility. No one challenge this point of view. Probably, it can be acknowledged that the freedom to use ICT is one of the basic human rights. However, there are political 'radicals' who place this right above all other human rights. One finds it difficult to connect with such an extremist approach, as well as with the formal statement of this right of free access. The freedom without proper accountability can be the one-way street to anarchy and lawlessness and it poses a threat of being self-detrimental. No freedom of access should be granted to criminals, terrorists and aggressors. On appearance it might look plain and clear. But anytime we intend to reflect this balance of freedom of and responsibility for the use of ICT in international documents, the tug of war of political controversies start to tighten. You can mention the freedom whereas you can't mention the responsibility. One notion is substituted for another: when nations exercise their right of sovereignty, they get vocal about censorship, in business relationships, etc.

This 'tug of war' is doubly counterproductive, since the mankind has learned to deal with the problem of giving the topic balanced treatment.

The famous International Covenant «On Civil and Political Rights» of December 19, 1966 explicitly states that the use of these rights carries with it special duties and responsibilities and may therefore be associated with some limitations: a) For respect of the rights or reputations of others b) For the protection of national security or of public order, or of public health or morals (Article 19).

Unfortunately, my counterpart made no mention whatsoever of responsibility for the use of ICT in his report. He puts the full-stop right away after the reference to freedom.

Second. Fueled by the United States and some of its partners, the issue of building capacity is gaining more popularity in political discussions on the international arena related to IIS matters in the last year and a half. Attempts are made to include it in G8 documents or in the UN Forum on Cybercrime, i.e. virtually anywhere possible.

Who objects to covering 'digital gap' and rendering appropriate technological assistance, especially to developing nations? Declarations alone will be of little use here. It is necessary and high time that this program should prepared in detail and doubts

should be removed as to whether it would meet its objectives answering the questions that we are accustomed to hearing in bilateral consultations with other nations.

Many of them voice their concerns that such assistance could turn into technological neo-colonialism; become a disguised form of lobbying individual producers, set some discriminatory standards of technological development; attach political conditions and adversely affect their sovereignty.

It is important to ensure that the assistance in the capacity building program, should not, on one hand, become a cover for interference in the internal affairs of recipient countries, and, that on the other hand, it should not give additional muscle to the «digital Frankenstein» ultimately, inflicting damage on donor countries, and that obtained know-how should not be used for illegal or malicious purpose.

Third, in the fight against cybercrime, the United States and European Union are actively imposing the legal scheme of tackling criminal problems in the field of ICT by globalizing the famous Budapest Convention 2001 passed by the Council of Europe. Over 12 years, it has been signed by 49 nations and ratified by 39 nations. An overwhelming majority of nations, including Russia, are skeptical, if not suspicious of it, and are not going join it.

In our view, this paper in essence «gives the green light» to interference in the internal affairs of other states and unauthorized access to their information space, ignoring their sovereignty in the information space. Also, the Convention is extremely outdated. According to experts, it treats as criminal only 9 instances of illegal use of ICT, while there are about 30 of them nowadays. It contains no concepts, such as cyber-terrorism or botnets, nor does it account for the realities of the legal systems in countries that are not included in the eligible, but very limited set of its original authors.

In order to combat on a global phenomenon such as cybercrime it takes rather than a highly partisan approach, a general and contemporary document drafted under the UN framework with unqualified participation of all nations, that would take into account every benefit of the Budapest convention and regional best practices and was not affected by their weaknesses and limitations.

Forth, quite a stir is being raised over whether international law applies to modern military and political conflicts in the information space, or relating to the use of ICT or it doesn't. It is very much unclear, inconsistent, if only because of the fact that the contemporary international law originated before the revolutionary breakthrough followed by the development and application of ICT and, accordingly, without regard to developments generated by this process.

From our perspective, rather than the formal declaration of the applicability principle, we should be looking at the principle of adapting international law to new

phenomena in the information/digital environment. Unmodified application of old rules to new developments may cause the opposite effect. Perhaps politicians and lawyers must urgently take up the job of developing new rules of law and definitions.

The main thing is to grasp the following: we all stand for prevention and control of a cyber-war and therefore for its legitimization. Russia unreservedly supports the first option. The second option leads to the notorious concept dating to the 60-es, the full swing of the Vietnam War, the so-called 'limited nuclear war or nuclear escalation' of armed conflicts, now applicable to the use of ICT.

For starters, one might think of cooperation on information security of critical infrastructures and the so-called confidence-building measures rather engaging in 'a tug of war' over the applicability of international law.

Fifth, the economic or financial side of IIS related to national security and social stability. It is known that the global and irreversible trend of economic development in the world is the migration of financial accounts to a virtual scheme of things and as a result complete removal of cash out of circulation.

It presents us with a challenging question – would the generally positive process of putting the economy on a non-cash basis lead to the new political super-goal which will be implemented according to the following formula: those control the use of ICT, are in control of the financial flows and therefore, the world politics? Will the next global redistribution of power within the oligarchic elite that ensures a position of superiority in the world economy prove to be a prelude to disasters, including those of military and political nature, where mankind will be made to act as a martyr as has repeatedly been the case in the history?

Let me give a specific example to show how it will work out in practice. Since you're all tired, I'll do it in such a way as to put a smile on your faces. When I came in Garmisch on this occasion, my friends and I went to a nearby store to buy something to celebrate this event. Due to technical reasons, the credit cards were not accepted and we failed to buy something that we needed. Here we have an example of social instability fraught with political consequences, especially, if such disruptions in the global economy are caused at someone's arbitrary will.

So, the simple conclusion is self-evident – the «asteroid» of our common global cyber-danger is on an approaching trajectory. We are losing time available to take political action for mutual protection. What needs to be done is stop pulling over the blanket or rope to your side and reach within a short span of time some specific international agreements on rules or principles of responsible behavior of states, on measures of trust in the information space, on prevention of an arms race and cyber confrontation that may put international peace and security to a very tough test.

Гельмут Хабермайер
(H. Habermayer)
Глава управления по военной стратегии,
координатор по вопросам кибербезопасности,
Министерство обороны и спорта Австрии

О ВЛИЯНИИ ВОЙН В КИБЕРПРОСТРАНСТВЕ НА ГРАЖДАНСКОЕ НАСЕЛЕНИЕ

Введение

В двадцать первом веке любое мало-мальски значимое событие реальной жизни, включая политические и военные конфликты, находит свое отражение в киберпространстве. Тех, кто занимается обеспечением национальной безопасности, в данном контексте волнуют пропаганда, шпионаж, терроризм и собственно военные действия. Суть угроз безопасности стран не изменилась, но благодаря Интернету атаки стали мощнее, быстрее и масштабнее. Их повсеместность и непредсказуемость означают, что сражения, которые ведутся в киберпространстве, не менее (и даже более) важны чем то, что происходит на реальном поле боя.

Непрерывная эволюция компьютерных технологий означает, что защищаться от цифровых атак едва ли станет легче. Нематериальность сетевого пространства делает любые расчеты относительно победы, поражения и боевых потерь крайне субъективными. Удивительное дело – даже факт нападения бывает довольно затруднительно установить. Большого количества информации в открытом доступе нет, крупных конфликтов между крупными военными державами после начала эпохи Интернета не наблюдалось, и неосведомленность большинства организаций по вопросам их собственной кибербезопасности заставляет встревожиться.[1]

[1] К. Гирс: раздел “Demystifying Cyber Warfare” в публикации Schröfl/Rajaeed/Muhr: “Hybrid and Cyber War as consequences of Asymmetrie”, (2011) П. Ланг, стр. 119

Растущая зависимость от информационных технологий (ИТ), а также от необходимой для их использования инфраструктуры превращает безопасное киберпространство в неотъемлемый элемент существования любого государства. В то же время достижения в сфере ИТ дали террористам и прочим нарушителям закона новые возможности для нападения, которые они все активнее используют. Примечательно, что киберпреступники используют одни и те же методы при разных целях и мотивах. Они учатся друг у друга и часто работают сообща.

Я попытаюсь продемонстрировать растущую зависимость от цифровой среды, а также расскажу о недавно возникших обстоятельствах, которые непосредственно связаны с угрозами, исходящими из цифрового пространства. В моей речи я также коснусь проблем, которые стоят перед людьми, занимающимися обеспечением кибербезопасности, и опишу аргументы в пользу развития и внедрения комплексного подхода к киберзащите. В конце своей речи я предложу варианты стратегий, которые в современных условиях могут оказаться интересными для тех, кто принимает ответственные решения в данной сфере.

Хотя людей, стоявших у истоков Интернета, нельзя упрекнуть в недальновидности, они и представить себе не могли, что их детище разовьется в глобальную коммуникационную инфраструктуру, которую мы по итогу имеем. С тех времен, когда Интернет использовался исключительно для передачи научных и военных данных, многое изменилось, и отчасти сегодняшние сложности с обеспечением безопасности и функциональности сети вызваны тем, что тогда, при зарождении сети, это не было насущной проблемой. Усилия были направлены на дублирование каналов связи, эффективность и совместимость. Так насколько же сильно мы зависим от киберпространства?[2]

О целях кибератак

Сетевая атака сама по себе не является целью. Это, скорее, незаурядное средство для решения множества задач. Цели атакующего в первую очередь ограничиваются его собственным воображением и наличием доступа к интересующей его сети. Ниже представлены пять вариантов целей, которые может преследовать нападающий и которые имеет смысл рассмотреть лицам, занимающимся обеспечением национальной безопасности, при формировании стратегии защиты.

[2] Н. Малисевич: раздел “Options for Tackling Current and Future Cyber Threats” в публикации Schröfl/Rajaeed/Muhr: “Hybrid and Cyber War as consequences of Asymmetrie”, (2011) П. Лэнг, стр. 187

Шпионаж

Лидеры государств все чаще заявляют об угрозе цифрового шпионажа («Отчет Коди по шпионажу» (“Espionage Report...» and Cody), 2007 г.). Ежедневно неизвестные хакеры крадут большие объемы данных, как из систем хранения, так и при передаче их по сети. По сути, полноценную сетевую разведывательную операцию можно скоординировать из любой точки планеты, даже если речь идет о хорошо засекреченной политической или военной информации.

Пропаганда

Простая, дешевая, эффективная и одна из самых мощных форм кибератак. Для пропаганды в сети взлом как таковой может вообще не потребоваться – достаточно преимущества естественной скорости распространения информации в Интернете. Цифровые данные, текст ли это или изображение, можно отправить в любую точку планеты, включая расположение противника, а их правдивость не имеет в данном случае абсолютно никакого значения. Кроме того, любой провокационный материал, удаленный из сети, может снова в ней появиться в течение нескольких секунд.

Атака на отказ в обслуживании (Denial-of-Service, DoS)

Идея DoS-атаки проста – ограничить использование информационного ресурса для рядовых пользователей. Самая распространенная практика – «утопить» целевой ресурс в таком количестве запросов, при котором он не сможет обслуживать обычных пользователей. Другие варианты атаки предусматривают физическое уничтожение оборудования и воздействие электромагнитным полем, результатом которого становятся скачки напряжения или силы тока, нарушающие работу электроники.

Модификация данных

Цель такой атаки – нарушение целостности исходных данных. Хитрость данного подхода заключается в том, что рядовой пользователь (как человек, так и роботизированная система) может принять важное решение на основании искаженных данных. Варианты атаки варьируются от «дефейса» веб-сайтов (от англ. defacement – «искажение, уродование»), который иногда также называют «цифровым граффити» с размещением пропагандистской информации или дезинформации, до ударов по базам данных с конечной целью нарушения работы оружейных систем и систем оперативного управления.

Перехват эксплуатации сетей инфраструктуры

Критически важные элементы инфраструктуры, как и все остальное, становятся все сильнее привязаны к Интернету. Тем не менее, в силу того, что в подобных системах часто используется практика моментального ответа на запрос, а вычислительных мощностей может не хватать для решения такой задачи, система безопасности может быть уязвима. Особое внимание в контексте обеспечения национальной безопасности имеет смысл уделить электросетям, поскольку замены электричеству не существует, а от него зависят все остальные элементы инфраструктуры (Divis, 2005 г.). Наконец, важно то, что почти все критически важные элементы инфраструктур находятся в ведении частных компаний. [3]

Критически важные элементы инфраструктуры – это объекты, работа которых играет важную роль в поддержании общественного благополучия. Их уничтожение или нарушение их работы имеет серьезные последствия для здоровья населения, его безопасности, экономического и социального благополучия или для нормальной работы правительства. При разработке плана по защите такого рода объектов необходимо осознавать их важность и использовать комплексный подход. Например, на основе Европейской программы по защите критически важной инфраструктуры Австрия разработала план, названный «Австрийская программа по защите критически важной инфраструктуры» (APCIP). Этот план описывает основные принципы программы, включая уровни приоритетности секторов, определение критериев для отбора критически важных элементов инфраструктуры, факторы риска и учитываемые тенденции, список мер по защите критически важной инфраструктуры, а также меры по разработке плана действий с расписанными подзадачами.

Общеевропейская программа насчитывает 11 секторов, в которых присутствуют критически важные элементы инфраструктуры: энергетика, ядерная промышленность, ИКТ, водоснабжение, продовольственный сектор, здравоохранение, финансы, транспорт, химическая промышленность, освоение космоса и организации, занятые в НИОКР. Работа всех значимых центров, узлов связи и управляющих систем данных секторов основана на информационно-коммуникационных технологиях и в значительной степени зависит от них, а управление может осуществляться лишь из определенных точек.

Для Австрии не все эти сектора имеют такое же значение, как для Евросоюза. Например, ядерная энергетика и космическая программа не являются самыми важными национальными интересами, тогда как поддержка

[3] К. Гирс: раздел “Demystifying Cyber Warfare” в публикации Schröfl/Rajaeed/Muhr: “Hybrid and Cyber War as consequences of Asymmetrie”, (2011), П. Лэнг, стр. 122

социальных и оборонных систем и организаций быстрого реагирования достаточно критичны. Австрия вступила в эпоху информационных технологий относительно быстрее чем, скажем, Эстония, и потому она сильнее зависит от критически важных элементов инфраструктуры. Это означает, что необходимо приложить значительные усилия для обеспечения безопасности таких объектов и принять комплексные меры их защиты.[4]

Выводы

Сама по себе кибератака при вооруженном конфликте не является динамической силой, не имеет физических характеристик и не жестока по своей природе, но этот факт не означает, что она не является объектом Международного гуманитарного права. Кибератаки вызывают все больше вопросов, поскольку они могут быть направлены, к примеру, на производственные ресурсы врага, его системы реализации продуктов или банковские объекты, а последствия таких ударов довольно сложно оценить. Принципы Международного гуманитарного права гласят, что гражданское население следует обезопасить, а ресурсы, необходимые для его благополучия и территории, на которых гражданские лица проживают, не следует подвергать ударам, и согласно этому принципу в контексте новых методов борьбы формируются базовые директивы. Вследствие этого после нескольких кибератак прошедшего десятилетия были слегка переработаны стратегические планы, но ни разу дело не закончилось смертельным исходом или нанесением значительного ущерба! Подготовка в более широком смысле этого слова может заключаться в защите критически важных (для жизнедеятельности населения) объектов инфраструктуры и конкретных мерах по обеспечению кибербезопасности.

Государство должно выделить ресурсы для создания инструментов анализа, оценки и прогнозирования тенденций в сфере информационно-коммуникационных технологий, что включает в себя анализ рисков, создание постоянного ситуационного центра для отслеживания и анализа потенциальных угроз, а также создание системы раннего оповещения и организаций аварийного реагирования (разного рода групп реагирования на чрезвычайные и кризисные ситуации).

Таким образом, любое государство, в значительной степени зависящее от информационных технологий, нуждается в создании централизованного органа, задачей которого является сбор и анализ информации на всех уров-

[4] В. Унгер: раздел “Cyber War and the Protection of Strategic Infrastructure” в публикации Schröfl/Rajaeed/Muhr: “Hybrid and Cyber War as consequences of Asymmetrie”, (2011), П. Лэнг, стр. 151

нях, включая данные, предоставляемые частными лицами. Такая организация должна, в частности, иметь полномочия на проведение разведывательных, превентивных, защитных и реакционных мероприятий или как минимум обязывать других лиц на подобные действия. Она также могла бы стать фундаментом для эффективного координирования действий, направленных на обеспечение кибербезопасности на федеральном и международном уровнях. Очевидно, впрочем, что для создания такой организации необходимо обеспечить соответствующую законодательную базу, учитывающую особенности отдельно взятой страны, а способ, выбранный для решения этой задачи, во многом обусловит подход к обеспечению кибербезопасности в будущем.[5]

[5] Там же, стр. 153

Helmut Habermayer
Ministry of Defence and Sports,
Head Military Strategy Division and Cyber Coordinator, Austria

EFFECTS OF CYBER WARFARE ON THE CIVILIAN POPULATION

Introduction

In the twenty-first century, everything significant that happens in the real world, including every political and military conflict, will also take place in cyberspace. For national security planners, this includes propaganda, espionage, terrorism, and even warfare itself. The nature of a national security threat has not changed, but the Internet has provided a new delivery mechanism that can increase the speed, diffusion, and power of an attack. Its ubiquitous and unpredictable characteristics mean that the battles fought in cyberspace can be just as important – if not more so – than events taking place on the ground.

The dynamic and constantly evolving nature of computing technology ensures that cyber defenses will never be easy to maintain. The intangible nature of cyberspace can make the calculation of victory, defeat, and battle damage a highly subjective undertaking. And amazingly, even knowing whether one is under attack can be a challenge. Much information lies outside the public domain, there have been no wars between two first-class militaries in the Internet era, and the ignorance of most organizations regarding the state of their own cyber security is alarming.[6]

Growing dependency on information technology (IT) and the interdependence of related critical infrastructures have made a secure cyberspace vital to the functioning of the modern state. At the same time, advances in the IT sector have also presented terrorists and other criminals with new opportunities and attack vectors that they are increasingly exploiting. Notably, perpetrators of cyber-crimes share common methods even if their goals and motivations differ. They learn from each other and frequently work together.

I will try to showcase how dependency on cyberspace is continuously increasing, and will outline recent developments as they pertain to threats emanating from cyberspace. It will point to related challenges for those tasked with keeping cyberspace safe and secure and argue that today's threats to cyber security can best be tackled

[6] K. Geers: "Demystifying Cyber Warfare" in Schröfl/Rajaeed/Muhr: "Hybrid and Cyber War as consequences of Asymmetrie", (2011) P. Lang, p 119 ff

by elaborating and implementing a comprehensive approach to cyber security. It will conclude by offering a few policy options for contemporary decision makers.

Although nobody can accuse the Internet's early developers of a lack of foresight, they could never have imagined that their invention would develop into the global communication infrastructure it is today. Still, much has changed since the Internet was first developed as a tool to share scientific and military information, and much of the challenge in keeping cyberspace safe, secure and functional derives from the fact that security was not a priority when the Internet was created. Instead, the focus was on redundancy, efficiency and interoperability. But, exactly how dependent on cyberspace are we, really?[7]

Cyber-attack Goals

A cyber-attack is not an end in itself. Rather, it is an extraordinary means to a wide variety of ends. The goals of a cyber-attack are primarily limited by the imagination of the attacker and his or her access to a target network. Here are five examples that national security thinkers should keep in mind as they incorporate cyber security into their defense strategies.

Espionage

Increasingly, world leaders publicly complain of the threat posed by cyber espionage ("Espionage Report...» and Cody, 2007). On a daily basis, anonymous computer hackers steal vast quantities of computer data and network communications. In fact, it is possible to conduct devastating intelligence gathering operations, even on highly sensitive political and military communications, remotely from anywhere in the world.

Propaganda

Cheap and effective, this is often the easiest and the most powerful form of cyber-attack. Propaganda dissemination may not need to incorporate any computer hacking at all, but simply take advantage of the amplification power of the Internet. Digital information, in text or image format – and regardless of whether it is true – can be instantly copied and sent anywhere in the world, even deep behind enemy lines. And provocative information that is removed from the Web can reappear in seconds.

[7] Malisevic: "Options for Tackling Current and Future Cyber Threats" in Schröfl/Rajaeed/Muhr: "Hybrid and Cyber War as consequences of Asymmetrie", (2011) P. Lang, p 187 ff

Denial-of-Service (DoS)

The simple strategy behind a DoS attack is to deny the use of data or a computer resource to legitimate users. The most common tactic is to flood the target with so much superfluous data that it cannot respond to real requests for services or information. Other DoS attacks include the physical destruction of computer hardware and the use of electromagnetic interference, designed to destroy unshielded electronics via current or voltage surges.

Data modification

This category of attack targets the integrity of data. It is insidious, because a successful attack can mean that legitimate users (human or machine) could make important decisions based on maliciously altered information. Such attacks range from website defacement (often referred to as "electronic graffiti," but which can still carry propaganda or disinformation) to database attacks intended to corrupt weapons or command-and-control (C2) systems.

Infrastructure manipulation

National critical infrastructures are, like everything else, increasingly connected to the Internet. However, because instant response is often required, and because associated hardware may have insufficient computing resources, security may not be robust. The management of electricity may be especially important for national security planners to evaluate, because electricity has no substitute, and all other infrastructures depend on it (Divis, 2005). Finally, it is important to note that almost all critical infrastructures are in private hands.[8]

Critical Infrastructures are those infrastructures, or parts thereof, which are of substantial relevance in maintaining important societal functions. Their disruption or destruction has serious effects on the health, security or the economic and social wellbeing of the population. or on the effective functioning of government. Plans for protecting such infrastructures should be cognizant of their importance and comprehensive in their approach. For example, on the basis of the European Program for Critical Infrastructure Protection, a national master plan was elaborated for Austria, called - the Austrian Program for Critical Infrastructure Protection (APCIP). APCIP describes the principles of the program, including listings of priority sectors; definitions of criteria for rating critical infrastructures; identifying risk factors and

[8] K. Geers: "Demystifying Cyber Warfare" in Schröfl/Rajaeed/Muhr: "Hybrid and Cyber War as consequences of Asymmetrie", (2011) P. Lang, p 122 ff

relevant actors; listing measures for the protection of critical infrastructures; and developing an action plan with detailed sub-goals.

The Europe-wide program lists 11 sectors of critical infrastructures: energy, nuclear industry, ICT, water, victuals, health, finances, transport, chemical industry, space travel and research institutions. The centers, communication nodes and steering systems of these critical infrastructures at the disposal of a modern society are based on information and communication technology or are of considerable importance for the ICT and can only be operated in certain locations.

For Austria not all of these sectors have the same relevance as they do for the EU. For example, nuclear industry and space travel are of no specific national importance, but conversely, emphasis is placed on constitutional installations, the maintenance of the social and defense systems as well as first responder organizations. Austria's transformation into the information age is relatively more advanced than that of Estonia, and therefore Austria depends even more upon the functioning of its critical infrastructures. This calls for great efforts in order to ensure and sustain their functioning by taking comprehensive security measures[9].

Conclusions

The fact that a computer network attack during an armed conflict is not kinetic, physical or violent in itself, does not put it beyond the remit of Intern. Humanitarian Law (IHL). Computer network attacks open up new questions since they can be used, f.e., against the enemy's production, distribution and banking systems, making the impact more difficult to judge. The IHL principle that civilians should be protected and their livelihoods and the environment in which they live should not be targeted, provides basic guidance when faced with these new methods of warfare. Some cyberattacks over the past decade have briefly affected state strategic plans, but none has resulted in death or lasting damage! Preparation in a wider sense can only be done in protection of critical (vital) infrastructure and concrete Cyber Defence measures.

The state has to provide adequate resources in developing a national means of analyzing, assessing and predicting developments in strategic ICT - including risk assessment, a permanent situation center for observation, estimates of the threat environment and, if necessary, for early warning, alert, and the activation of reactions and emergency organizations (such as CERT/CSIRT, or Computer Emergency Response Team/ Computer Security Incident Response Team).

[9] W. Unger: "Cyber War and the Protection of Strategic Infrastructure" in Schröfl/Rajaeed/ Muhr: "Hybrid and Cyber War as consequences of Asymmetrie", (2011) P. Lang, p 151 ff

Thus, what any state with a high degree of dependence on IT today needs is a central body to collect, analyzes, and assesses all pertinent information from government agencies at all levels as well as from private parties. This organization should also have the authority to take the necessary reconnaissance, prevention, defense, and reaction measures, or at least obligate other assets to do so. This authority would also ensure underpin the effective steering and coordination of national and international cooperation regarding cyber war. Clearly however, the necessary legal preconditions for such a body would have to be established and tailored in each national context and the manner in which this is accomplished may well affect the way in which individual states can defend themselves against cyber war threats in the future[10].

[10] Ibid, p 153 ff

Мирошников Б.Н.
Институт проблем
информационной
безопасности
МГУ им.Ломоносова

ТРИ ТЕЗИСА О ПРОБЛЕМАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Добрый день, уважаемые коллеги! Я глубоко признателен организаторам за приглашение принять участие вот уже в седьмой Конференции. Очень важно, что мы регулярно собираемся здесь, где поднимаются и обсуждаются актуальнейшие проблемы безопасности в киберпространстве. Нисколько не боюсь преувеличить огромное значение такой Конференции, потому что, во-первых, все мы видим, насколько обостряется проблема обеспечения информационной безопасности в глобальном масштабе, и, во-вторых, сегодня как никогда важен голос ученых, экспертов и специалистов, способных выработать стратегические решения и рекомендации, которые позволят снизить уровень напряженности и опасности в информационном пространстве планеты и превратить его в цивилизованную, безопасную и удобную среду, служащую человечеству.

Хочу поблагодарить и первого, и второго выступающего. Интересно, компетентно и познавательно. Однако у меня сложилось впечатление, что все-таки эти выступления были, в некоторой степени, академичны и как-то спокойны. И мне показалось, что надо «добавить перцу», как-то обострить ситуацию и предложить первый тезис: «МЫ ОПОЗДАЛИ ИЛИ МЫ ОПАЗДЫВАЕМ». Угроза расползается по всему миру с огромной скоростью, а на фоне этой динамики наше «вялотекущее и благостное» совещание только констатирует и всячески демонстрирует эту динамику.

Великолепные натовские и европейские программы, интересные совещания на разных солидных уровнях – Интерпол, Европол, ОБСЕ, пленумы, форумы и так далее, на которых видно, какие усилия предпринимаются человечеством

для защиты от киберугроз. Однако из года в год мы дружно констатируем, что преступность выросла, что ущерб он нее также возрастает в разы. Это может означать лишь одно – что предпринимаемые до сих пор меры не дали искомого результата – снижения киберугрозы и, наоборот, повышения уровня безопасности существования человека в киберпространстве планеты. Увы!

На нашей Конференции, на других национальных и международных форумах сегодня можно слышать огромное количество разнообразных данных, характеризующих угрожающую динамику развития киберугроз и, в частности, киберпреступности. Количество вирусов, вредоносных программ, количество пораженных объектов, суммы нанесенного ущерба, суммы похищенных денег, количество зараженных компьютеров, скомпрометированных пластиковых карт, размеры бот-сетей, количество ДОС-атак, размеры спамового потока и так далее, и так далее. Не буду утомлять Вас приведением этих цифр – их будет еще много. А еще будет много процентов – на сколько все это выросло! То есть страшную картину мы дружно рисуем и с ней согласны.

Вопрос главный – насколько достоверны эти данные? Уверяю Вас, они очень приблизительные и отличаются от действительных, как правило, в меньшую сторону. За исключением тех, что получены методом произвольной экстраполяции. Этим стали грешить многочисленные исследователи, среди которых попадаются и самодеятельные, которые отсутствие достоверной информации заменяют фантазией и умозрительными заключениями, сделанными исходя из зачастую эгоистических соображений. Например, антивирусные компании, как правило, дают более высокие статистические данные по вредоносным программам и ущербе, чем, скажем, правоохранительные органы. Первым нужно напугать общественность и заставить покупать свой продукт, вторым – показать свою работу и снизить недовольство общества своими скромными результатами. Подобные мотивы сильно влияют на статистику, которую затем специалисты включают в свои исследования, отчеты и доклады. Поэтому, когда мы используем и, тем более, предъявляем где-нибудь статистические данные, рекомендую обязательно указывать источник их происхождения. Уже такое указание позволит применить к этим данным соответствующий коэффициент достоверности.

С другой стороны, понятие «киберпреступность» до сих пор в разных странах и у разных исследователей имеет очень размытые границы. В результате одни и те же деяния в одних странах попадают в таблицу ИТ-преступности, в других – в экономические или просто уголовные преступления, а в третьих - вообще не криминализованы. Помножьте или прибавьте к этому

традиционную латентность компьютерной преступности и получим размытую акварель в тревожных цветах, вокруг которой происходят наши бдения.

Так что предлагаю второй тезис – «НАУКА ПО-ПРЕЖНЕМУ В ДОЛГУ!» Для развития науки в ее прикладном значении для целей усиления мировой информационной безопасности сегодня существует много благоприятных условий, чем это было, скажем, когда мы здесь собирались на первую конференцию в 2007 году.

Во-первых, накоплено огромное количество фактографического материала, который доступен для обработки и научного объективного, неангажированного и неполитизированного осмысления.

Во-вторых, накоплен и также доступен разнообразный опыт (положительный и отрицательный) организации противодействия киберугрозам, киберпреступникам, кибертеррористам и киберэкстремистам, а также опыт межгосударственного взаимодействия. Хочу подчеркнуть – и отрицательный! Чрезвычайно важно изучать не «передовой опыт», а именно ошибки, просчеты и недостатки – из такого исследования рождаются затем реальные позитивные рекомендации и решения.

В-третьих, созданы и работают многочисленные научно-исследовательские коллективы в различных учебных и научных центрах, а также в государственных и негосударственных учреждениях, в бизнес-сообществе. Выросли профессиональные кадры, специализирующиеся на изучении киберугроз и информационной безопасности.

В-четвертых, благодаря, в том числе, и таким международным мероприятиям, как наша конференция, в мире созревает понимание необходимости активного, честного международного сотрудничества для исследования всего комплекса проблем, связанных с обеспечением МИБ – международной информационной безопасности. Пример – созданный в 2010 году Консорциум, который с радостью принимает новых членов для объединения интернациональной научной мысли, озабоченной будущим человечества в новых реалиях информационного века.

Это очень хорошо и правильно, объективно созрело, ибо ученые, занимающиеся своим важным делом в своих странах изолированно друг от друга, в итоге подобны строителям вавилонской башни. Как известно, говорящие на разных языках, они не сумели ее построить.

Поэтому вновь и вновь приходится говорить о необходимости приведения к общему знаменателю терминологии – понятийного аппарата для воз-

можности проведения сравнения и анализа данных в глобальном масштабе, а завтра - и на временной оси. До тех пор, пока на одном конце планеты будут мерить в дюймах, а на другом - в метрах или килограммах, достоверной картины информационных угроз в мире мы не нарисуем.

Мысль далеко не новая, и на открытие я не претендую. Об этом мы говорим на всех концах света уже много лет подряд. Но проблема далеко не решена, и именно ученые в союзе с практиками должны, наконец, составить единый словарь общеупотребимых и однозначно понимаемых терминов в области информационной безопасности и всех составляющих известной триады МИБ. Легкий, но яркий, на мой взгляд, пример. На русском языке наши отечественные специалисты затрудняются разъяснить принятый и распространенный на Западе англоязычный термин «компьютерный саботаж». А этот термин во многих странах вошел даже в их уголовные кодексы.

В чем же дело? Почему мы опаздываем? Почему мы по-прежнему, несмотря на глобальный Интернет и практически неограниченные возможности общения, говорим на разных языках, как вавилонские строители? По-моему, человечество до сих пор не осознало степень опасности того джина, которого оно выпустило в свое электронное пространство. И того факта, что это пространство сегодня обладает совершенно уникальными качествами, как замечательными, так и таящими многие угрозы, осознанные или еще нет.

И это при том понимании, что само по себе существование этого информационного пространства - цифровой оболочки планеты, есть новая цивилизационная ступень в развитии общества. А на этой новой ступени появляются элементы новой экономики, новые социальные отношения, в том числе и правоотношения, новые стратегии, в том числе и военные. Специалисты, ученые понимают и видят то, чего еще не осознает остальная часть человечества. В частности то, что темпы развития этой среды значительно опережают темпы развития мер по защите человека и общества от угроз, исходящих из нее.

Специалисты понимают и вроде бы не молчат, однако их не слышит общество всеми своими частями. Взять, к примеру, бизнес – самая активная, прогрессивная, состоятельная часть общества. Очень прогрессивный сектор. Бизнес во многом способствует развитию телекоммуникационных систем, осваивает киберпространство, внедряя электронную торговлю, например, стремится к расширению своего абонентского «ареала», стремится к извлечению максимальной прибыли. Однако на фоне этой гонки бизнесу еще предстоит осознать свою социальную ответственность, прислушаться к специалистам и направить свои усилия и капиталы на безопасность. К сча-

стью, уже и сегодня есть примеры положительного отношения отдельных представителей капитала к насущным проблемам информационной безопасности. Но их мало, примеров другого рода намного, к сожалению, больше.

Обращается банк к киберполицейским: Помогите, нас обокрали кибермошенники. Скимминг, кардинг и так далее. А уже через неделю начинают жаловаться: они не приняли никаких мер, не нашли преступников, не вернули деньги. Не знают и не хотят знать, что таких заявлений у киберполицейских три десятка в неделю. А самих полицейских в два раза меньше. А расследование каждого эпизода занимает немало сил, средств и времени.

Затем киберполицейские обращаются в банк за информацией о прохождении преступных денег по счетам. Через неделю в ответ получают лекцию о банковской и коммерческой тайне и охране персональных данных. И никаких справок. Работа остановилась без всяких шансов на продолжение. Преступников никто не ловит и никогда не поймает. Ситуации почти типовые.

Правоохранительные органы и спецслужбы говорят о регистрации пользователей информационных систем и некотором регулировании, хотя бы в части негативного контента. В ответ визг правозащитников, Интернет-сообщества в лице блогеров и других активистов, обвинения в тотальном контроле и так далее. А речь-то идет всего лишь о том, чтобы правоохранительные органы могли лучше выполнять свою функцию – защиты граждан своей страны от преступников, террористов, защиты детей от растлителей, извращенцев.

Известно, каким мусором забит Интернет, причем не просто мусором, а преступным содержанием, вроде террористических, экстремистских, порнографических и прочих подобных сайтов. Однако многочисленные обращения правоохранительных органов к руководству интернет-провайдеров по-прежнему не имеют результата. Понятно, для фильтрации и чистки контента им придется серьезно потратиться. Тогда нужен другой механизм – Закон, который урегулирует эти отношения и позволит на законных основаниях бороться как с авторами и распространителями нежелательного (преступного) контента, так и с теми, кто делает вид, что не замечает его под собственным носом. Надо признать, что в последнее время государством начали приниматься меры по очищению (хотя бы частичному) Интернет-пространства – Роскомнадзор формирует списки сайтов, подлежащих закрытию и требует от провайдеров выполнения их предписаний. Однако мы видим, с каким трудом проходили эти решения, с каким трудом осуществляются эти меры, какое сопротивление они вызывают. А что, Роскомнадзор сам себе придумал работу? Разве это не то, что требовали граждане, разве это не требование здравого смысла, выраженное негодованием гражданского общества?

Ведомства и Службы глухи друг к другу. Вместо поиска ошибок в работе у соседа хорошо бы понять, в чем его (партнера) трудности и постараться помочь.

Отсюда позвольте предложить следующий тезис или лозунг – «СЛЫШАТЬ ДРУГ ДРУГА!» Оказывается, это большая проблема. Мы не слушаем и не слышим друг друга, мы мало учитываем ситуацию, трудности и возможности партнера, того, с кем мы обречены быть в одной лодке и вместе выживать.

Приведу пример. Читаю отчет о конференции, посвященной безопасности бизнеса и борьбе с мошенничеством. Что говорят участники, и кто они, эти участники? Представители банковского сообщества, представители общественных объединений – банковского союза и союза платежных систем, неистовый и вездесущий народный депутат… Перепроверяю: а где представители правоохранительной системы, которым приходится ловить, разоблачать кибермошенников, отдавать их в руки правосудия? Оказывается, их там не было. Может быть, их приглашали, а они не пришли? – Нет, их просто не пригласили. Зато все участники бойко поговорили о захлестнувшей страну киберпреступности, эпидемии кибермошенничества и дружно выразили общее мнение о недееспособности киберполиции. И никто не спросил, а почему так происходит? А чем, может быть, помочь? Нет желания услышать партнера, понять, что ему мешает или что ему нужно. А, казалось бы, общая цель должна объединять. Но если на низком уровне взаимодействия чего-то не видно, то должен существовать верхний координационный уровень, который видит и управляет. Ученые, исследователи должны помочь такому управленческому звену владеть ситуацией и подсказывать решения.

Та же ситуация, но намного сложнее для преодоления - в секторе международного взаимодействия по обеспечению международной информационной безопасности в целом и, в частности, по борьбе с киберпреступностью. Киберполицейские одной страны обращаются к киберполицейским другой страны: дайте логи, протоколы соединений, дайте владельцев IP-адресов, номеров сотовых телефонов и так далее. Любому понятно, что расследование ИТ-преступлений требует по определению быстрых, практически немедленных действий. Если не остановить преступную транзакцию, миллионы уйдут в цифровой туман и там быстро растворятся. В киберпространстве события происходят молниеносно и так же молниеносно исчезают следы, улики, доказательства, если их быстро не зафиксировать. Очевидно, что так же быстро должно осуществляться взаимодействие между соответствующими структурами – между службами банковской безопасности, между операторами связи и провайдерами Интернета, между полицейскими подразде-

лениями, расследующими киберпреступления. А что в ответ? – Пожелание коллегам оформить международное следственное поручение. Мол, у нас сложные внутригосударственные процедуры. А надо понимать, что в России международное следственное поручение оформляется исключительно через Генеральную прокуратуру. И многим уже не раз объясняли, что это означает весьма и весьма продолжительное время. Тем не менее – ответа нет, преступники ликуют, никто их не ловит.

Понятно, в разных странах существуют разные подходы к выдаче информации, разные режимы хранения и получения информации – теми же полицейскими от банков или операторов связи. Однако эти режимы имеют отношения к правилам, сформировавшимся в XX веке, когда не было единой общедоступной интернациональной информационной среды безо всяких границ. Первые, кто этим пользуется, это международные компьютерные преступники. А мы до сих пор не создали законных правовых механизмов для оперативного реагирования и взаимодействия, соответствующего скоростям и реалиям XXI века. А граждане планеты никак не могут осознать, что нападение на их компьютер, на локальную сеть их фирмы, завода или больницы возможно из любой точки этой планеты!

Что мешает? Ведомственные интересы, групповой эгоизм, конкуренция, межгосударственные противоречия, и даже противоречия внутри законодательной базы, не говоря уже о международной.

Мы пытаемся что-то делать на уровне национальных контактных пунктов. Напомню, что национальные контактные пункты созданы еще в конце девяностых по решению глав правительств наших стран и существуют в более чем 40 странах. Но реально этот механизм работает, когда сотрудники по обе стороны границы знакомы друг с другом, знают, кто и чем занимается. Это глубоко неправильно, но это факт. Зачастую они руководствуются целесообразностью, как там они ее понимают от смены к смене, а не законом и инструкцией, вытекающей из закона.

К сожалению, наши законы отстают от стремительных процессов, происходящих в информационной среде, от возникающих новых правоотношений, в которые втянуты как отдельные граждане, так и целые группы, социальные среды. Это понятно. Известно, право консервативно и инерционно. Событие должно произойти, повториться, стать явлением. Мы должны его изучить, выявить его влияние, скрытые в нем противоречия, чтобы затем выйти с нормативными регулирующими актами либо законами.

Но мы с Вами, будучи «на гребне волны», находимся как раз в той пограничной зоне, когда старые законы уже устарели, а новых пока еще не создали. И от нас зависит скорейший приход того, чего, может быть и неосознанно, от нас ждут народы наших стран. Давайте работать. Это «сладкое бремя» – быть впереди, понимать больше, чем понимают другие, брать на себя ответственность и находить решения.

Не скрою, хотелось бы принять участие в очередной конференции в Гармиш-Партенкирхене, а, может быть, и выступить хотя бы на 1 минуту. И успеть предложить следующие тезисы – после сказанного здесь «слышать друг друга» предложить – «ПОНИМАТЬ ДРУГ ДРУГА», а затем – «ПОМОГАТЬ ДРУГ ДРУГУ!»

Успехов Вам и всем нам, уважаемые коллеги!

B.N.Miroshnikov
Institute of Information Security Issues,
Lomonosov Moscow State University

THREE THESES ON INFORMATION SECURITY ISSUES

Good afternoon, dear colleagues, I am deeply grateful to the organizers for inviting me to the seventh Conference. It is of utmost importance that we gather on a regular basis here where the most urgent issues in the cyberspace security are raised and discussed. I am not concerned in the least that I might exaggerate the importance of this Conference, because, firstly, we can see how the problem of information security is escalating on a global scale, and secondly, it is critical today, more than ever, to have the mouthpiece of scientists, experts and professionals capable of working out strategic decisions and recommendations that will scale down the level of tension and danger in the information space in the world and turn it into a civilized, safe and comfortable environment serving the needs of humanity.

I would like to thank both the first and second speakers. Compelling, expertly done and informative. However, I have a feeling that all these presentations have been, in a sense, academic and somehow laid-back. And it has seemed to me that it is necessary to 'add some spice', somehow ruffle up things and offer the first point: WE HAVE BEEN LATE OR ARE BEING LATE. The threat is spreading around the world at a fast pace, and while it is at it, our 'easy-going and blissful' meeting only is in stark contrast to and in every way indicative of this process.

Excellent NATO and European programs, interesting meetings at various levels of authority like Interpol, Europol, OSCE, plenary sessions, forums, and so on, – they are showcases of efforts that are being undertaken to protect humanity against cyber threats. However, every year we unanimously state that crime rate has risen increasingly multiplying its detrimental effect. This can only mean one thing – that the measures that have been undertaken so far has gone wide of the target, i.e. to reduce the cyber threat and, as a result, improve human safety in the cyberspace world. Alas!

At this Conference as well as at other national and international forums today you can get an enormously wide variety of data showing an alarming growth record of cyber threats, in particular, cyber crimes. The number of viruses, malware applications and affected facilities; the amount of damage and stolen money; the number of infected computers and compromised cards; the size of botnets, the number of DOS attacks, the volume size of the spam flows and so on and so forth.

I will spare you the details – there will be many more. And there will be many percentages showing by how much it has grown! In other words, a terrible picture is revealed to us here and we put up with it.

Here is the main question as to how accurate this data is. I assure you, they are very rough estimates and normally differ from actual figures to the lower side, except those derived by the random extrapolation method. These falsehoods started to come forth from a large number of researchers, including amateurs who substitute the lack of reliable information for fantasies and speculations often based on self-serving considerations. For example, anti-virus companies normally provide higher statistics on malware and the resultant damage than, say, law enforcement agencies. The first group needs to scare the public and make them buy their products, the second group – to show their work and appease public grudge by downplaying the existing threats. Such motives strongly affect statistics that are further included by experts in their studies, reports, and presentations. Therefore, when using such data, and, moreover, citing statistics somewhere, I recommend you should always make reference to the original source. Even such reference would treat such data with an appropriate degree of trust.

On the other hand, the concept of «cybercrime» is still extremely vague in different countries and with different researchers. As a result, the same wrongdoings in some countries are classified as IT crimes, in other countries –or as economic crimes or criminal offenses, and yet in some countries – are not treated as something liable to criminal prosecution. Multiply this by or add it to the traditional latency of computer crimes and what you get is a blurred watercolor picture in alarming colors which is the subject of our debates.

So I am putting forward my second point that "SCIENCE STILL OWES US!" Today, there is a more favorable environment to advance science so that it can be applied for the purpose of strengthening global security than it was, say, when we gathered here in the first conference in 2007.

First, we have built up a massive evidential base that is available for review and interpretation from a fair-minded, non-partisan and non-political perspective.

Second, we have gained and can tap into the varied experience (positive and negative) of organizing the fight against cyber threats, cyber criminals, cyber-terrorists and cyber extremists, and the experience of intergovernmental cooperation. I would like stress that there is a negative experience as well! What does require study on the top priority basis is not 'best practices', but specifically, mistakes, errors and faults and it is this kind of study that produces genuinely positive recommendations and solutions.

Third, a multitude of research groups have been set up and operating at various educational and research centers, as well as government and private institutions and in the business community. The army of professionals specializing in the research of cyber threats and information security has also been formed.

Fourth, thanks, in particular, to international events such as this conference, the world is getting aware of the need for active and straight international cooperation in studying the entire range of problems associated with IIS, i.e. international information security. As an example I can refer to the Consortium established in 2010, that is willing to admit new members in order to organize the international scientific school of thought concerned about the future of mankind in the new realities of the information age.

It's very positive and correct with the scene set for it for obvious reasons as scientists pursuing their important research in their respective countries in isolation from each other, are ultimately like builders of the Tower of Babel. As you know, people speaking different languages, they have not managed to build one.

So again and again we have to speak of the need to agree on the common terminology, concepts and references to aid the comparison and analysis of data on a global scale, and tomorrow – within the present timeframe. As long as at one end of the planet measurements will be made in inches, and at the other - in meters or kilograms, we will not be able to draw an accurate picture of information threats in the world.

The idea is not a new one and I do not claim to the authorship. This is what we have been talking about in all parts of the world for many years running. But the problem is far from being solved, and scientists in conjunction with practitioners should finally produce the single vocabulary of commonly used and clearly understood terms in the field of information security and all components in the well-known triad of IIS. There is, I believe, an easy, but illustrative example. In Russian, our local experts find it difficult to interpret the English term 'computer sabotage' adopted and broadly used in the west. And in many countries this term became part of their national criminal codes.

What's the matter here? Why are we late? Why are we still, despite of the global Internet and almost unlimited possibilities of communication, speaking in different tongues, like Babylonian builders? In my opinion, humanity has not yet realized the level of hazard that it has released in its electronic space. And the fact that today this space has altogether unique qualities both outstanding and those concealing many threats, identified and yet to be discovered.

And with the understanding that the mere existence of the information space – the digital envelope of the planet – there is a new civilization stage of society development. And at this new stage there are emerging elements of new economy, new social relationships, including the legal relations, new strategies, including military ones. Experts and scientists understand and perceive what has not yet dawned upon the rest of humanity. In particular, the fact that the pace of development in this sphere is significantly outrunning that measure building to protect individuals and society from threats emanating from it.

Experts understand and counsel on those things with society and all its parts remaining aloof. Take, for example, business – the most active, advanced and affluent part of society. It is a promising sector. For the main part due to the development of telecommunication systems business develops the cyberspace, by introducing e-commerce and seeking to expand its customer range and to maximize its profits. However, with this race going on in its back yard, businesses has yet to become aware of its social responsibility, to heed expert advice and channel its efforts on and capital to security. Fortunately, today there are already examples of the positive attitude from individual representatives of capital owners to the pressing problems of information security. But they are few such examples and, unfortunately, there are far more examples of the opposite kind.

A bank contacts a cyber police department: Help, we have been robbed by cyber fraudster. Skimming, carding, and so on. A week later they are starting to complain: they failed to take any action, find any criminals and get our money back. Yet they neither know, nor do they care to know that three dozens of such requests are filed with this cyber police department every week. And the staff of police officers is a third of this number. And an investigation of each crime element takes a lot of time, effort and resources.

In turn cyber police officers turn to the bank for information on movements of illegitimate money in the bank accounts. A week later they get lectured on banking and commercial secrecy and protection of personal data. And no statements are given. This work stopped dead in its track without any chances to continue. No one is trying to catch criminals and will never catch anyone. Situations are nearly 'boiler plate'.

Law enforcement and intelligence agencies insist on user registration in information systems and some regulation, at least, as applicable to the negative content. In response to squeals from human rights advocates, the Internet community represented by bloggers and other activists lashed back with accusations of total control and so on. And what needs to be done is only to enable law enforcement agencies to perform their functions more efficiently, i.e. protect their citizens from criminals and terrorists and protect children from child molesters and perverts.

It is well known how weltered the Internet is, not just with spam, but with criminal content such as terrorist, extremist, pornographic and other similar websites. However, repeated appeals from law enforcement agencies to Internet providers' administrations have drawn a blank. Clearly, it will cost arm and leg to them to filter and clean the content. Then another mechanism is required, i.e. the law that will regulate these relationship and will allow legal fight against both authors and distributors of undesired (criminal) content and also those who pretend not to notice it under their own noses. One should admit that the government has recently started taking some steps to clean up (at least partially) the web space – Roskomnadzor generates lists of websites to be closed and requires providers to follow their instructions. However, we see what obstacles these decisions have met and are meeting and what resistance is put up to confront them. And it isn't Roskomnadzor that set itself on this job, is it? Is not that what has been required by citizens and common sense and voice by civil society resentment?

Agencies and Services are unresponsive to one another. Instead of picking faults with your partner, it would be sensible to understand what difficulties it is saddled with and try to be of help.

Hence, let me propose the next point or motto – "LISTEN TO EACH OTHER!" It turns out to be a big problem. We do not listen to and cannot hear each other, we give little consideration to the situation, challenges and opportunities of a partner, someone with whom we are destined to be in the same boat and survive.

I will give an example. I am reading a report of the conference on business security and fraud fighting. What do participants say and who are those participants? Representatives of the banking community, public associations – the banking union and the union of payment systems, as well as running wild and omnipresent MPs .... I am double checking: and where are representatives of the law enforcement system who have to track and expose cyber fraudsters and hand them over to justice? It turns out that they have not been there. Maybe they were invited but failed to come? – No, they were not invited. But all the participants spoke volumes about the cybercrime epidemic hitting the nation and amicably shared the view of the cyber police's inability to handle its job. And no one asked why it was happening this way? How can it be helped? There is no desire to hear a partner, to understand what holds it back or what he needs. And, it looked as if the common goal should have brought them together. But if nothing can be seen at a low level of interaction, there must be an upper level of coordination that can see and control things. Scientists and researchers should facilitate this management team to control the situation and prompt solutions.

The sector of international cooperation on international information security in general and on the fight against cybercrime, in particular, has the same situation, but much more challenging one to tackle. Cyber police officers of one country turn to their counterparts in other countries: please give us logs, connection protocols as well as details on owners of IP addresses, cell phones and so on. It is plain to anyone that the investigation process of IT crimes, by definition, requires rapid and almost immediate actions. Unless you stop the criminal transaction, millions will go under the digital fog and vanish in thin air. In the cyberspace, events take place at a lightning speed with traces clues and evidence disappearing as fast unless you get a quick fix on them. Apparently interaction between the relevant bodies: between bank security services, operators and Internet providers and between police units investigating cyber crimes. What do we have by way of response? - A recommendation to colleagues to file an international investigative request. Well, you have complex domestic procedures. And we must understand that in Russia international investigative request is filed exclusively through the General Prosecutor's Office. And many have repeatedly explained that this means a very, very long time. However there is no response, criminals triumph and no one try to catch them.

Naturally, different countries have different approaches to provision of information, different information storage and retrieval conditions – as applicable to relations between police officers and banks or operators. However, these conditions are related to the rules that were formed in the XX century, when there was no single generally accessible international information environment without any boundaries. The first people to capitalize on it are international computer criminals. And we have not yet created any legitimate legal procedures for rapid response and interaction matching the pace and actual requirements of the XXI century. And the citizens of the planet simply cannot understand that an attack on their computer and the local network of their firm, factory or hospital can be mounted from anyplace around the globe!

What's the snag? Departmental interests, group egoism, competition, inter-state conflicts and even contradictions within the domestic legal framework, to speak nothing of international law.

We are trying to do something at the level of national contact points. Let me remind you that national contact points are set up in the late nineties by the decision of the heads of our national governments and are available in more than 40 countries. But actually, this scheme of things works when the staff on both sides is on personal terms with each other and knows who does what. This is profoundly wrong, but it's a fact. Often, they are guided by what they see reasonable from shift to shift, rather than by the law and a procedure stemming from the law.

Unfortunately, our laws are lagging behind rapid processes ongoing in the information environment and new emerging legal relations involving individuals, entire groups and social communities. It is understood. It is known, law is conservative and inertial. The event should take place, happen again and become a phenomenon. We have to learn to identify it, its impact and contradictions concealed within it then in order to put together governing regulations or laws.

But you and I, being "on the crest of a wave," are just in the border region where the old laws are outdated, and the new ones have not yet been drafted. And it is down to us to deliver as early as possible what is unknowingly expected of us by our compatriots. Let's continue our work. This is a 'sweet' burden to step ahead, understand more than others do, take on responsibility and find solutions.

To be honest, I would like to attend the next conference in Garmisch-Partenkirchen and, perhaps, to speak for at least 1 minute and to have the opportunity after what I have said 'hear each other' to offer the following points –'UNDERSTAND EACH OTHER' and then - 'HELP EACH OTHER'!

Good luck to you and all of us, dear colleagues!

Д-р Чарльз Барри (Charles L. Barry)
Центр исследований политики
в области технологий
и национальной безопасности
Национальный университет обороны США

ВЗГЛЯД НА НАЦИОНАЛЬНЫЕ И МЕЖДУНАРОДНЫЕ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ

Введение

Настоящий документ описывает академическую точку зрения на проблемы киберпространства национального и международного уровня. Цель автора – внести свой вклад в международный диалог в относительно недавно сформировавшейся теме обеспечения кибербезопасности. В первой части статьи будут описаны нынешние угрозы информационной безопасности по всему миру. Вторая часть сосредоточена на описании национальных и международных подходов к решению проблемы в краткосрочной и долгосрочной перспективе. В качестве примера отдельно взятой страны использованы Соединенные Штаты, тогда как усилия НАТО по обеспечению безопасности своих сетей рассматриваются как образец международного сотрудничества. США и НАТО стали движущей силой развития безопасного Интернета, посредством которого осуществляется львиная доля передачи данных, как защищенных, так и открытых. Но, несмотря на положение их как центральных фигур, Соединенные Штаты и Альянс – это только одна из стран и одна из организаций среди множества сильных игроков. Следовательно, приведенные примеры следует рассматривать как собирательные образы игроков в сфере, в которой нормы поведения как таковые пока не выработаны. Документ описывает видение американского аналитика. Для формирования комплексного подхода к обеспечению кибербезопасности следует принять во внимание и другие точки зрения.

Раздел I. США и международная кибербезопасность

Главным элементом борьбы США за безопасное будущее сети остается «Международная стратегия США для киберпространства» 2011 года.[11] Это основополагающий документ, поддерживающий три принципа: свободу самовыражения, неприкосновенность частных данных, а также свободный доступ к информации. «Стратегия» соответствует основной цели США: «глобальной работе по развитию открытой, легкодоступной, безопасной и надежной ИК-инфраструктуры, которая поддерживала бы международную коммерческую деятельность, обеспечивала бы должный уровень безопасности и поощряла самовыражение и использование новейших технологий».[12]

«Международная стратегия США для киберпространства» полностью соответствует мнению о том, что существующие международные нормы мирного поведения и разрешения конфликтов вполне применимы и в киберпространстве, признавая при этом, что следует поработать для того, чтобы понять, как и в каком виде эти нормы следует применять. Таким образом, эти нормы следует привязать к традиционным принципам поддержки фундаментальных свобод, уважения права частной собственности, права на сохранение тайны личных данных, права на защиту от правонарушителей, а также права на применение средств самозащиты. Именно на этом фундаменте стоят международные нормы, перечисленные ниже:

- Глобальная совместимость систем
- Стабильность сети
- Надежный доступ к сетевым ресурсам
- Многостороннее управление
- Обеспечение кибербезопасности усилиями государств[13]

В «Стратегии» описываются три основных вектора, которых придерживаются США в отношении обеспечения кибербезопасности: улучшение международных дипломатических отношений, отражение и предотвращение нападений посредством улучшения систем защиты, а также содействие всеобщему процветанию и безопасности посредством инвестиций в их развитие.

---

[11] Полное название майской публикации 2011 года- International Strategy for Cyberspace - Prosperity, Security and Openness in a Networked World. См. веб-сайт Белого дома: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

[12] Там же, стр. 8.

[13] Там же, стр. 10.

В «Стратегии» также подробно раскрываются 7 приоритетных направлений развития безопасного, надежного и доступного Интернета, которыми занимаются США:

• продвижение международных стандартов и поддержка открытых рынков в целях экономического роста;

• повышение безопасности, надежности и отказоустойчивости глобальных сетей;

• развитие сотрудничества в правоприменительной сфере и обеспечение соблюдения законов;

• готовность вооруженных сил к противостоянию угрозам в киберпространстве;

• создание эффективных структур управления Интернетом;

• наращивание возможностей повышения безопасности и процветания;

• Построение в Интернете системы фундаментальных свобод и прав на частную собственность.

Вышеприведенный план относится к выпущенной более двух лет назад в США комплексной дорожной карте, описывающей развитие политики взаимодействия с электронной средой для каждого ведомства. Она же является базой для развития программ кибербезопасности и показывает, как именно США видят будущее безопасного и эффективного Интернета.

За прошедшее время было запущено несколько программ, нацеленных на внедрение этой стратегии, с учетом усиления описанных угроз. Во многих отношениях рост угроз стимулирует рост количества инициатив по обеспечению безопасности. В 2012 году США поддержали проекты ООН (описаны ниже), усилия ОБСЕ и НАТО, нацеленные на поиски компромиссов в отношении вопросов безопасности.

В феврале 2013 года Белый дом издал указ, устанавливающий процедуры повышения защищенности критических объектов инфраструктуры. Данный указ – хорошая возможность для сторонних лиц получить представление о комплексном взаимодействии многочисленных федеральных агентств по вопросам кибербезопасности, начиная с Министерства внутренней безопасности[14], Министерства торговли, Министерства обороны, Министерства юстиции и заканчивая такими органами как Административно-бюджетное

[14] Для получения информации о роли, которую Министерство внутренней безопасности играет в сфере решения вопросов кибербезопасности см. «A Civil Perspective on Cyber Security,» авторы – Джейн Холл Льют и Брюс Макконнелл, от 14 февраля 2011 г., журнал Wired. См. http://www.wired.com/threatlevel/2011/02/dhs-op-ed/.

управление и Федеральное бюро расследований. И это одни из немногих защитников государственной инфраструктуры[15]. Эти же службы ответственны за налаживание связей со своими зарубежными коллегами и координирование вопросов кибербезопасности (от правоприменения до стандартов совместимости).

Активное и эффективное участие в международной работе

Формой продвижения своей позиции является участие в работе форумов, многонациональных институтов и двусторонних встреч. Представители Соединенных Штатов присутствуют практически на каждом международном форуме по кибербезопасности, как от госструктур, так и частного сектора и академических учреждений. За прошедшие годы самые разные представители США побывали и на Международном форуме в немецком Гармише-Партенкирхене, который становится все более значимым мероприятием.[16] Официально США принимает участие в международных мероприятиях гораздо чаще, чем кажется. В 2011 году представители Государственного департамента приняли участие в форуме ОБСЕ по обеспечению конфиденциальности информации и принятию мер по повышению кибербезопасности,[17] чиновник Министерства торговли является членом консультативной группы при Форуме ООН по управлению Интернетом.[18] Вице-президент США принял участие в лондонской конференции по нормам поведения в киберпространстве.[19] В 2012 году Соединенные Штаты участвовали в будапештской конференции по проблемам киберпространства, а сейчас их представители готовятся к треть-

[15] Также в феврале в Конгресс был подан законопроект под названием Cyber Intelligence Sharing and Protection Act (касавшийся нелегального контента в Интернете), предполагалось, что он будет одобрен к концу года. См. публикацию Николь Блейка Джонсона «Support for Info Sharing Could Speed Cyber Law» («Поддержка обмена информацией может ускорить принятие закона о кибербезопасности), C4ISR Journal, июнь 2013 г., стр. 9.

[16] Полное название форума 2013 IISI - «The Seventh International Forum for Partnership of State Authorities, Civil Society and the Business Community in Ensuring International Information Security.» Он организуется и проводится Институтом проблем информационной безопасности МГУ им. М. В. Ломоносова, спонсором также является ICANN и некоторые частные организации.

[17] См. замечания Кристофера М. Пейнтера, координатора от США по проблемам киберпространства при Государственном департаменте, от 9 мая 2011 г. См. http://www.osce.org/cio/77482

[18] См. http://www.intgovforum.org/cms/component/content/article/121-preparatory-process/1290-mag-2013.

[19] См. http://www.whitehouse.gov/photos-and-video/video/2011/11/01/vice-president-biden-delivers-remarks-london-conference-cyberspace.

ему мероприятию, инициатором которого выступает Великобритания – конференции в Сеуле в октябре 2013 года.

На данный момент существуют три основные державы в контексте разрешения проблем кибербезопасности – это Китай, Россия и Соединенные Штаты. Не секрет, что эти страны отличаются как по своим позициям в вопросах безопасности, так и по степени открытости Интернет-пространства (помимо прочих позиций). Несмотря на разницу в подходах, каждая из стран регулярно взаимодействует с двумя другими в рамках ряда мероприятий. Эти три страны постоянно участвуют в большинстве международных форумов по кибербезопасности. Примерами таких мероприятий являются лондонская, будапештская и сеульская конференции, упомянутые выше. А самая, вероятно, высокая прозрачность работы наблюдается в Группе правительственных экспертов ООН (ГПЭ ООН), которая встречается для обсуждения тенденций информационно-телекоммуникационной сферы в контексте международной кибербезопасности.[20]

По инициативе России, ГПЭ ООН, насчитывающая 15 стран-участников, встречалась в рамках нескольких мероприятий в 2004, 2009-10 и 2012-13 гг. для рассмотрения угроз киберпространства. По итогам первой встречи единый отчет не был составлен, хотя после второй серии заседаний участники достигли компромисса по некоторым рекомендациям.[21] Нынешняя серия встреч завершается в июне 2013 года. Если договоренность по содержанию итогового отчета будет достигнута, его передадут в Генеральную Ассамблею до конца 2013 года. Важно отметить, что соглашения ГПЭ отражают единую позицию не только пяти постоянных членов Совбеза ООН, но также Германии, Индии и многих других стран, играющих важную роль в вопросах кибербезопасности[22]. Несмотря на то, что деятельность ГПЭ нередко воспринимается как малозначимая и имеющая существенные ограничения, их позиция отражает максимально возможный на данный момент уровень взаимопонимания

[20] См. www.un.org/disarmaments/topics/informationsecurity. Кибер- и информационная безопасность находится в компетенции Первого комитета Генеральной Ассамблеи ООН. Работа проводится под наблюдением Управления ООН по вопросам разоружения.

[21] Второй раунд заседаний Группы правительственных экспертов проводился под председательством посла РФ Андрея Крутских, имевшего полномочия представителя пяти постоянных членов Совбеза ООН, а также проявившего личный энтузиазм при проведении переговоров. См. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N10/469/57/PDF/N1046957.pdf?OpenElement.

[22] Помимо пяти постоянных членов Совбеза, Германии, Индии, Беларуси и Эстонии, членами GGE в 2009-10 2012-13 гг. стали другие страны.

по вопросам кибербезопасности и, таким образом, ее необходимо учитывать при разработке новых соглашений.

В апреле 2013 г., после продолжительных переговоров, Соединенные Штаты и Китай условились о создании рабочей группы для обсуждения вопросов кибербезопасности. Основным вопросом, волнующим США, являлась растущая уверенность в том, что сетевой шпионаж с целью кражи интеллектуальной собственности американских компаний (в том числе работающих на оборонную промышленность) ведется китайцами, конкретно – китайскими оборонными службами. Китай, в свою очередь, обеспокоен доступностью «недолжной» информации для рядовых пользователей своей страны, что потенциально снижает авторитет правительства. Американо-китайская рабочая группа по вопросам кибербезопасности провела первые встречи в июле, в рамках пятого американо-китайского стратегического и экономического диалога в Вашингтоне.[23]

Еще большее значение придается соглашению между США и Россией по мерам, направленным на снижение риска киберконфликта, готовому к подписанию Президентами Обамой и Путиным на саммите большой восьмерки в Великобритании 17 июня 2013 г. Соглашение, в рамках которого в течение нескольких месяцев будет создана двусторонняя рабочая группа, аналогичная американо-китайской, также предусматривает создание трех формальных каналов взаимодействия между американскими и российскими службами. Первый – это «горячая линия» между координатором США по вопросам кибербезопасности и его российского коллеги для прямой связи в кризисные моменты. Второй канал задействует Национальный центр США по уменьшению ядерной опасности, построенный в 1987 г. для оповещения населения о ядерной угрозе, в качестве центра оповещения о проведении учений, которые могут быть восприняты как атака, а также центра по повышению осведомленности в случае, если таковые атаки со стороны другой страны имеют место быть. Третий формальный канал – это прямой обмен техническими данными (например, IP-адресами, с которых идет вредоносный трафик) между американской Группой быстрого реагирования на компьютерные инциденты при Министерстве внутренней безопасности и их российскими коллегами.[24]

[23] См. http://www.nbcnews.com/technology/us-china-agree-work-together-cybersecurity-1C9337442 и http://thenextweb.com/insider/2013/04/13/china-and-the-united-states-will-create-a-joint-working-group-to-deal-with-cybersecurity/

[24] Эллен Накашима, статья «U.S., Russia Agree to Set Up Computer Security Link» («США и Россия договорились строить отношения в сфере компьютерной безопасности»), Washington Post, материал от 18 июня 2013 г., стр. 10.

Ясно, что, несмотря на зачастую противоположные взгляды, но в силу резкого усиления угрозы, идущей из киберпространства,[25] Китай, Россия и США делают большие шаги на пути к созданию норм поведения, которые призваны снизить международное напряжение и выступить в качестве модели для прочих стран.

Помощь другим странам в обеспечении кибербезопасности

Неотъемлемой частью американской политики, изложенной в «Международной стратегии для киберпространства», является повышение осведомленности других стран о возможных рисках, а также развитие их механизмов защиты от угроз электронной среды, особенно тех, которые зарождаются внутри их собственных границ.[26] Помощь включает консультации по защите сетей, обучение и сертификацию специалистов по кибербезопасности, создание первичных групп быстрого реагирования и наращивание ресурсов в сетевых операционных центрах и службах безопасности центров обработки данных.

Министерство торговли, Министерство обороны, а также частные университеты и компании продолжают работу с правительством Афганистана по многим из перечисленных проблем.[27] США также оказывают помощь в рамках двусторонних отношений с членами НАТО и развивающимися странами по всему миру, поскольку эти страны выразили интерес в повышении собственного уровня кибербезопасности. Логика такого взаимодействия проста: любая незащищенная зона Интернета – это риск для всех остальных сетевых ресурсов. Таким образом, чем глобальнее защита, тем безопаснее Интернет для всех, кто его использует.

Обучение людей, готовых к противостоянию угрозам

Еще один ключевой аспект работы США в контексте обеспечения кибербезопасности – это обучение будущего поколения, которое должно иметь иммунитет к угрозам электронной среды. Этот элемент программы Мини-

[25] Для получения информации о напряженном взаимодействии чиновников США и Китая по вопросам кибершпионажа на встрече IISS Shangri-La Dialogue в Сингапуре (которая состоялась 1 июня 2013 года), см. материал Эрнесто Лондоно “Hagel chides China for cyberspying, which draws rebuke from a general” («Хейгл упрекает Китай в шпионаже и вызывает ответную критику со стороны генерала»), статья в Washington Post от 2 июня 2013 года, стр. A15.

[26] Международная стратегия для киберпространства», май 2011 г., стр. 15 («Наращивание мощностей киберзащиты»).

[27] Поддержкой деятельности в Афганистане с 2004 года занимается консультационная группа по вопросам телекоммуникаций при Министерстве обороны (ISAF).

стерства внутренней безопасности называется Stop-Think-Connect («Остановись, подумай, подключайся»). Соединенные Штаты участвуют в обучении значительного количества будущих высококвалифицированных специалистов, занятых как в частном секторе, так и на государственной службе. Эти люди смогут адекватно противостоять проблемам, связанным с надежностью, безопасностью и отказоустойчивостью Интернета, и смогут защитить информацию, передаваемую посредством его инфраструктуры.

Ключевая образовательная инициатива Национального научного фонда – программа Cyber Watch («Электронный дозор»), которая начала свою работу в 2005 году в виде сообщества 10 организаций, действующих на территории Вашингтона, округ Колумбия. Сегодня это федеральная программа, в рамках которой задействовано 29 штатов и сотрудничают 50 муниципальных колледжей и 45 университетов, предлагающих прошедшим обучение возможность получить степень и участвовать в технических и нетехнических соревнованиях, относящихся к электронной среде. Более 40 частных компаний, государственных организаций и ассоциаций задействовано в данной программе, а среди прошедших ее – более 500 преподавателей, работающих в организациях-участниках. В рамках Cyber Watch было разработано несколько учебных программ по обеспечению сохранности информации, предусматривающих сертификацию и получение научных степеней в сфере кибербезопасности на всех уровнях университетских структур. Относительно недавно в рамках Cyber Watch была налажена работа со школами. Cyber Watch – это самая многообещающая американская образовательная программа, призванная подготовить поколение талантливых и высококвалифицированных специалистов для противостояния угрозам киберсреды.[28]

Еще одна очень важная образовательная инициатива выдвинута Агентством национальной безопасности для университетов и колледжей, решивших получить статус Национальных центров передового опыта в сфере кибербезопасности. Данная инициатива имеет жесткие критерия разделения участников по трем направлениям: двухлетняя программа обучения, четырехлетняя программа с получением степени, и участие в научно-исследовательской деятельности в сфере кибербезопасности. На 2013 год 166 колледжей получили статус Центров передового опыта как минимум в одной из перечисленных категорий.[29]

---

[28] См. http://www.cyberwatchcenter.org/index.php?option=com_content&view=article&id=50&Itemid=29.

[29] См. http://www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml.

Раздел II. НАТО и кибербезопасность – данные за 2013 год[30]

Кибербезопасность впервые привлекла внимание НАТО на уровне первых лиц государств в 2002 году, вскоре после того, как Альянс впервые подвергся кибератаке. С тех пор руководство НАТО не забывает о противостоянии угрозам электронной среды. Лидеры стран-членов НАТО пришли к выводу, что кибератаки могут достичь такого масштаба, при котором они начнут угрожать процветанию, безопасности и стабильности как отдельных государств, так и всего Евро-Атлантического альянса. Агентства, командования, учебные центры и штабы Альянса ведут последовательную работу по предварительному обнаружению и подавлению атак, разработке сценариев восстановления систем после нападений. За последние 12 лет кибербезопасность стала высоко институционализированным направлением работы внутри Альянса и его процессов, включая ключевые вопросы составления оборонительного плана НАТО.

В 2013 году Организация Североатлантического договора (НАТО) продолжает наращивать мощности, необходимые для защиты своих внутренних сетей от растущего количества ежедневных проникновений, угрозы рассекречивания данных по причине пользовательской небрежности, а также плотного потока внешних кибератак. В начале июня министры обороны стран-членов НАТО провели первую встречу, посвященную исключительно вопросам кибербезопасности, что стало признанием растущего беспокойства в Организации. Усиление защиты сетей Альянса до конца 2013 года было признано приоритетным направлением. Также министры обратились к сотрудникам НАТО с просьбой к октябрю составить отчет о том, как именно Альянс может помочь своим странам, если они подвергаются кибератаке.[31]

Основной интерес НАТО в контексте кибербезопасности – защита тех сетей, которыми Организация владеет и которые эксплуатирует. Будучи именно альянсом, НАТО рассматривает кибербезопасность, как проблему национальную, а не как общую задачу для всех членов. Альянс не хочет, чтобы какая-либо из стран-участников оказалась зависима от его ресурсов и сократила свои инвестиции в кибербезопасность. Несмотря на то, что основное внимание Организации уделяется именно обороне, как отмечено в упомянутом выше отчете, специалисты НАТО пытаются определить, могут

[30] Для получения подробной информации по этой теме см. http://www.act.nato.int/.

[31] См. http://www.nato.int/cps/en/natolive/news_101143.htm. Это сводный отчет новостей с первого дня двухдневной встречи министров обороны стран-членов НАТО, проходившей 4-5 июня 2013 года.

ли они чем-нибудь помочь странам, которые запрашивают содействие в выстраивании адекватных ответных мер при кибератаках. Цитируя Генерального секретаря НАТО Андерса Расмуссена: «Для кибератак границ не существует. Для нашей защиты их тоже быть не должно».[32]

Эффективное управление средствами кибербезопасности в НАТО

Процессами электронной обороны, как и всеми другими действиями НАТО, управляет Североатлантический Совет. В 2011 году Совет приступил к исполнению решений стран-участников НАТО, принятых на саммите в Лиссабоне в 2010 году. Эти решения подразумевали создание новой концепции электронной защиты, новой политики и нового плана действий – все они были одобрены Советом к июню 2011 года.

Будучи масштабной сферой деятельности, кибербезопасность требует внимания всех стран-участников Альянса – их представители встречаются в рамках работы Управления по защите от киберугроз. Ежедневные процессы управления программами выполняются Международным штаб-секретариатом, в частности, Агентством киберзащиты при Директорате по новым проблемам безопасности. Другой важной структурой является Секретариат штаб-квартиры НАТО по консультациям, командованию и управлению. Это сводная группа, собранная из представителей Международного штаб-секретариата (в основном гражданские) и Международного военного штаба (в основном военнослужащие). Эти сотрудники наблюдают за обеспечением киберзащиты штаб-квартиры и других подразделений НАТО.

Управление систем связи и АИС НАТО (NCIA) занимается, помимо прочего, технической организацией киберзащиты. Одним из подразделений данной службы является Координационный центр по реагированию на компьютерные инциденты (NCIRC), который является внутренним эквивалентом Группы быстрого реагирования (CERT) для Альянса – это основной ресурс мониторинга сетей на предмет проникновения и определения других рисков, способных повлиять на деятельность организации.

Есть еще два элемента, которые играют ключевые роли в обеспечении кибербезопасности: Союзное командование операций ОВС (ACO) отвечает за командование всеми боевыми силами, и эксплуатирует большинство сетей, которые необходимо защитить; Союзное командование по трансформации (ACT) отвечает за выполнение большинства пунктов плана действий по обеспечению киберзащиты. Некоторые инициативы, относящиеся к плану их действий, описаны ниже чуть подробнее.

[32] Там же.

Страны-участники Альянса, как уже было сказано, изначально несут ответственность за собственную кибербезопаность. Тем не менее, в зонах, где сеть НАТО и национальные сети стран-участников взаимодействуют, Альянс настаивает на соблюдении ими технических и процессуальных стандартов Организации в отношении защиты данных (в частности, секретных данных).

Роль Союзного командования по трансформации НАТО

СКТ (АСТ) – это вестник перемен внутри НАТО и одновременно интеллектуальный капитал, который пригодится в будущем. Это командование отвечает за международные аспекты преобразований, проходящих в государствах, с учетом требований Альянса по международной совместимости. Такую роль командование выполняет как в контексте обеспечения кибербезопасности, так и в рамках всех других миссий и направлений. Таким образом, СКТ отвечает за работу, нацеленную на усиление позиций Альянса в киберпространстве в краткосрочной и долгосрочной перспективе. Основная задача СКТ – развитие (международное) концепций и доктрин Альянса, а также развитие образовательных программ и планов учений. Все эти сферы деятельности относятся в равной мере как к кибербезопасности, так и к любому другому аспекту обороны.

Еще одна важная работа – управление развитием потенциала НАТО в контексте кибербезопасности. Начинается она с выполнения требований, которые уже согласованы, но не внедрены в полной мере. СКТ также занимается долгосрочным планированием адекватности имеющихся ресурсов для противодействия будущим киберугрозам. При планировании будущих потребностей командование учитывает накопившийся опыт и оценивает эффективность имеющихся ресурсов.

СКТ отвечает за развитие концепций и доктрин НАТО в отношении осведомленности о мерах киберзащиты, ведя образовательную работу в учреждениях Альянса и распространяя методику обучения на школы стран-участников. В соответствии со своим планом в 2013 году НАТО обновляет свою методику и совершенствует программы обучения. По окончании данного процесса эти продукты будут рассмотрены штаб-квартирой Альянса и его странами-участниками. Как и все учебные материалы, информация по обеспечению кибербезопасности будет предоставлена в Военный комитет НАТО для одобрения.

СКТ также взаимодействует со сторонними организациями, с целью использования промышленных и научных экспертных знаний, которые могут понадобиться при разработке решений проблем, связанных с кибербезопасностью. У Альянса имеется прекрасно отлаженная программа взаимодействия с промышленным сектором, который теперь также включает в себя

технологии киберзащиты. Что касается использования научных ресурсов, то НАТО работает над их совершенствованием, решая такие задачи, как распределение ответственности при обеспечении киберзащиты или определение зависимости стран-участников Организации от внутренних коммуникационных и информационных систем.

Центр передового опыта по совместной защите от киберугроз[33]

Центр, расположенный в эстонском Таллинне, лишь недавно отпраздновал пятилетие и продолжает наращивать ресурсы и увеличивать масштаб деятельности. 11 стран-участников Альянса уже стали спонсорами данного центра, и еще 2 объявили о планах стать спонсорами.[34] Даже не являясь формальным подразделением НАТО, Центр - важный игрок в команде киберзащиты Организации. СКТ отслеживает деятельность всех Центров мастерства и передового опыта, аккредитуя их согласно стандартам Организации, а также привнося свою лепту в их программы. На данный момент готовится программа для Центра на 2014 год.

Миссия Центра передового опыта по защите от киберугроз заключается в развитии потенциала, сотрудничестве и обмене информацией внутри НАТО посредством образовательных и исследовательских программ, а также изучении опыта и консультациях. Цель Центра – стать основным источником экспертной информации в контексте совместной киберзащиты, накапливая, создавая и распространяя знание внутри Организации, а также среди ее стран-участников и партнеров. Три направления, по которым Центр ведет работу: вопросы юридического и политического характера; вопросы, связанные с обучением; исследования и разработки.

Центр разработал внушительный ежегодный план научных публикаций, технических курсов, конференций и учений. В частности, в 2013 году Центр успел составить «Отчет о состоянии киберзащиты в первом квартале 2013 г.» (First Quarter 2013 Cyber Security Status Watch report); в апреле он провел ежегодные сетевые учения Locked Shield («Поднятый щит»), а в июне - ежегодную конференцию CyCon.

---

[33] См. веб-сайт по адресу https://www.ccdcoe.org/3.html.

[34] Центры передового опыта, будучи вне структуры НАТО, тем не менее формируются и спонсируются странами-участниками Альянса. 11 стран, входящих в CCD COE: Эстония, Германия, Венгрия, Италия, Латвия, Литва, Нидерланды, Польша, Словакия, Испания и Соединенные Штаты. Франция, Турция и Великобритания также объявили о своих планах стать спонсорами.

Выводы

За последние 18-38 месяцев был отмечен значительный рост количества хорошо скоординированных атак на правительственные и частные сети. Данная тенденция показывает возросшее внимание к сети как основному средству нападения в попытках достичь политических, социальных и криминальных целей. Предполагается, что данная тенденция продолжит развиваться, пока международное сообщество не придет к консенсусу относительно норм поведения в киберпространстве. Атакующие могут быть преступниками, они могут являться представителями государств или действовать самостоятельно. Даже при отсутствии четкого представления об источнике атаки, его можно приблизительно определить, исходя из целей этой атаки. Усиление защиты – дело рядовых пользователей сети, будь то отдельные граждане, частные компании или административные учреждения. Все они должны позаботиться об ужесточении мер безопасности.

Соединенные Штаты двигаются по нескольким направлениям для усиления собственной защиты, учитывая при этом срочность, которая возникла после повышения частоты атак в мире. Планируется повышение защиты всей онлайн-активности в стране, и распространяться это будет на правительственные организации, частные компании, некоммерческие объединения, сообщества, а также на отдельных граждан. В данном контексте особое внимание Министерство обороны и Министерство внутренней безопасности уделят доменам .mil и .gov. В целом, основные усилия будут направлены на охрану критических объектов инфраструктуры. Цель Соединенных Штатов – это будущее поколение, которое хорошо информировано о возможных рисках более тесного взаимодействия с сетью. США активно участвуют во всех возможных начинаниях, относящихся к выстраиванию международной структуры законов и норм, которые помогали бы обитателям киберпространства. И, наконец, США заинтересованы в насаждении культуры открытой и безопасной сети.

НАТО организованно внедряет ряд комплексных программ по защите их собственных сетей. Будучи альянсом из 28 стран, НАТО уделяет большое внимание эффективности управления сетью и ее защиты. Результаты работы НАТО в плане создания организаций, заключения соглашений и раз-

вертывания защитных технологий – яркий масштабируемый пример того, что международное сообщество может достичь в масштабах всей планеты.

Отказ от ответственности.

Д-р Чарльз Барри
является независимым советником и старшим научным сотрудником Университета национальной обороны.
Мнения, выраженные в этой статье, принадлежат автору и не обязательно отражают политику Национального университета обороны, Министерства обороны или правительства Соединенных Штатов.

Charles L. Barry
Senior Research Fellow,
Center for Technology and National Security Policy (CTNSP)
NDU, USA

PERSPECTIVES ON NATIONAL & INTERNATIONAL CYBER ISSUES

Introduction

This paper provides an academic perspective on national and international cyber issues. The intent is to add to the wealth of international discourse on the emerging field of cyber security. The paper seeks to achieve this goal by first reflecting on the current state of threats to cyber security across the globe. Second, it will look at some of the national and international positions being taken to put in place near as well as long term cyber security. The national focus is primarily on the stated policies and positions of the United States, and the international focus is on NATO efforts to defend its own networks. These are the actors that have been central in advancing the security of the Internet, over which most communications and information, both open and secure, flows. Notwithstanding their centrality, the United States and NATO are but one nation and one international organization among many strong and capable actors in the global cyber domain. Therefore this reflection is couched in the broader context of a constellation of actors in a domain that is as yet without broad consensus on norms of behavior. It is the perspective of an American analyst. Other critical perspectives must be taken into account in order to distill a holistic appraisal of cyber security.

Part I. The U.S. and Cyber Security in the International Arena

The centerpiece of U.S. international engagement on cyber security for the future continues to be the 2011 International Strategy for Cyberspace.[35] This pivotal document espouses a commitment to the three principles of freedom of expression, privacy, and open access to information. It identifies a U.S. goal of «…work[ing] internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters freedom of expression and innovation.»[36]

[35] The full title of the May 2011 publication is International Strategy for Cyberspace - Prosperity, Security and Openness in a Networked World. See the White House website at

http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

[36] Ibid. Pg 8.

The U.S. International Strategy for Cyberspace endorses the understanding that long standing norms of international behavior in peace and conflict also apply in cyberspace, while accepting that work is needed to clarify how these norms apply and where they will need to be supplemented. Norms therefore should be grounded in the traditional principles of upholding fundamental freedoms, respect for property, valuing privacy, protection from crime, and the right of states to engage in self defense. Based on these values the U.S. supports the emerging international norms of:

- Global Interoperability
- Network Stability
- Reliable Access
- Multi-Stakeholder Governance
- Cyber Security Due Diligence by States[37]

The Strategy goes on to describe three primary lines of U.S. effort on cyber security: strengthening international partnerships through diplomacy; dissuading and deterring attacks through strong defenses; and, furthering global prosperity and security by investing in development.

The Strategy also elaborates seven policy priorities being pursued by the United States to realize a future Internet that is secure as well as reliable and open and interoperable:

- Promotion of international standards and open markets for economic growth
- Enhancing the security, reliability and resiliency of global networks
- Extending collaboration on law enforcement and the rule of law
- Military preparedness to deal with the security challenges of cyberspace
- Promotion of effective and inclusive Internet governance structures
- Building capacity, security and prosperity
- Furthering the cause of fundamental freedoms and privacy via Internet freedom

As the above outline shows, the U.S. elaborated, more than two years ago, a comprehensive roadmap for policy development by all departments as they engage in cyber space activities. It provides the basis for developing cyber security programs. It also points to the U.S. vision for a peaceful, dependable and productive future Internet.

[37] Ibid. Pg 10.

Since that time a number of programs have been initiated to implement this strategy even as the threats already described continue to gain momentum. In many ways the rapid growth of threats is fueling new security initiatives. In 2012 the United States supported work at the United Nations (described below), at the Organization for Security and Cooperation in Europe, and at NATO – to cite three of many international efforts – intended to coalesce international consensus on cyber security matters.

As already noted above, in February 2013 the White House issued its Executive Order (EO) establishing procedures for improving the cyber security of critical infrastructure. The EO is a useful document for outsiders to gain an impression of the complex interaction of the many federal agencies involved in cyber security, from the Departments of Homeland Security,[38] Commerce, Defense, and Justice to agencies such as the Office of Management and Budget and the Federal Bureau of Investigation. These are but a few of the major government participants in infrastructure protection.[39] These same departments each play a role in connecting to their international counterparts in other nations to coordinate on matters of cyber security, from law enforcement to interoperable standards.

Active and Robust International Engagement

A common theme of international implementation is engagement, whether in existing forums, multinational institutions or bilateral meetings. Indeed the United States is represented in almost every international forum on cyber security, either officially, by representatives of the private sector or by academic experts. All these types of representation have been present over the years at the IISI International Forum in Garmisch-Partenkirchen, Germany, which is steadily gaining prominence.[40] Official U.S. government participation takes place more often than realized. U.S. State Department officials participated in the 2011 OSCE forum on confidence and security[41] building measures for cyber security, and

[38] For a good perspective on the role of DHS in cyber security see «A Civil Perspective on Cyber Security,» by Jane Hall Lute and Bruce McConnell, 14 Feb 2011, Wired Magazine. Available at http://www.wired.com/threatlevel/2011/02/dhs-op-ed/.

[39] Also in February, the related Cyber Intelligence Sharing and Protection Act was reintroduced in Congress, with an expectation it will become law before the end of the year. See Nicole Blake Johnson, «Support for Info Sharing Could Speed Cyber Law,» C4ISR Journal. June 2013. Pg 9.

[40] The long title of the 2013 IISI forum is «The Seventh International Forum for Partnership of State Authorities, Civil Society and the Business Community in Ensuring International Information Security.» It is organized and hosted by the Institute for Information Security Issues, Lomanosov Moscow State University, and co-sponsored by ICANN and various private sector businesses and organizations.

[41] See for example remarks by Christopher M. Painter, U.S. Coordinator for Cyber Space Issues, Department of State, 9 May 2011 at http://www.osce.org/cio/77482.

a Commerce Department official is a member of the UN Internet Governance Forum's Multi-Advisory Group[42]. The U.S. Vice President participated in the London Conference on cyber space norms.[43] In 2012, the U.S. participated in the Budapest Conference on Cyberspace, and it is preparing to join the third in this series of UK-initiated conferences, the Seoul Conference in October 2013.

The three most significant powers in global cyber security issues are China, Russia and the United States, and it is no secret these powers differ in their policy positions on the security and openness of the Internet, among other issues. Notwithstanding their differences all three powers maintain regular dialogue with the others in a variety of relevant venues. All three participate regularly in most international forums on cyber security. One example would be the London, Budapest and Seoul conference trilogy just cited. Perhaps the highest visibility venue is the United Nations Group of Government Experts (UNGGE) that meets on «Developments in the Field of Information and Telecommunications in the Context of International Security.»[44]

The result of a Russian initiative, the 15 nation UNGGE has met over three series of events, in 2004, 2009-10, and in 2012-13, to consider threats from the cyber sphere. The first meeting did not result in an agreed report, however the second set of meetings did agree a report on several policy recommendations.[45] The current series of meetings concludes in June 2013. If a report can be agreed it is to be delivered to the General Assembly before the end of 2013. It is important to note that GGE agreements reflect the consensus among not only the five permanent members of the UN Security Council but also Germany, India and many other major powers, plus other important powers well known on cyber issues.[46] Although the results of the GGE is sometimes regarded as weak and limited thus far, it represents the current state of agreed consensus on cyber security at the

[42] See http://www.intgovforum.org/cms/component/content/article/121-preparatory-process/1290-mag-2013.

[43] See http://www.whitehouse.gov/photos-and-video/video/2011/11/01/vice-president-biden-delivers-remarks-london-conference-cyberspace.

[44] See www.un.org/disarmaments/topics/informationsecurity. Cyber or information security is a topic under the purview of the First Committee of the UN General Assembly. It is overseen by the UN Office of Disarmament Affairs.

[45] The second UNGGE round was chaired by Russian Ambassador Andrey Krutskihk, who had the stature as a UNSC Permanent Five member's representative as well as the personal drive to negotiate an agreed report. See http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N10/469/57/PDF/N1046957.pdf?OpenElement.

[46] Other than the five permanent UNSC members, Germany, India, Belarus and Estonia, the membership of the 2009-10 and 2012-13 GGE's has been comprised of different powers.

highest level and thus is important to note in seeking to advance new agreements.

In April 2013, the United States and China, after much negotiating, reached an agreement to establish a working group to discuss cyber security concerns. The key issue for the United States has been a growing conviction that cyber espionage aimed at stealing intellectual property from U.S. firms, including defense industry firms, have been traceable to China, and specifically the Chinese military. China is concerned over what is perceived to be inappropriate information being made openly accessible to online users in China, potentially undermining government authority. The U.S.-China working group on cyber security matters is to hold its first meeting in July, in conjunction with the fifth annual U.S.-China Strategic and Economic Dialogue in Washington.[47]

Even more significant will be the landmark U.S.-Russia agreement on measures to reduce risk of cyber conflict, signed by Presidents Obama and Putin at the UK hosted G-8 Summit on 17 June 2013. The agreement, which calls for standing up 'within the next month' a bilateral working group similar to the U.S.-China working group, also establishes three formal channels between U.S. and Russian counterparts. The first is a 'hot line' between the U.S. cyber security coordinator and his or her Russian counterpart to allow for direct communications in time of crisis. The second is to use the U.S. Nuclear Risk Reduction Center built in 1987 for nuclear warnings, to be used now to warn each other of cyber exercises that might be mistaken for attacks, and to raise inquires when perceived attacks appear to emanate from the territory of the other party. The final formal channel being agreed is the direct sharing of technical information, such as IP addresses suspected of emitting malicious traffic, between the U.S. Computer Emergency Readiness Team at the Department of Homeland Security and its Russian counterpart.[48]

What is clear is that despite sometimes sharply differing views and perhaps in part due to rapidly growing concerns over malicious activity in cyber space,[49] China, Russia and the United States are taking substantial and tangible steps toward establishing norms of behavior that will reduce tensions and serve as a model for other powers.

---

[47] See http://www.nbcnews.com/technology/us-china-agree-work-together-cybersecurity-1C9337442 and also http://thenextweb.com/insider/2013/04/13/china-and-the-united-states-will-create-a-joint-working-group-to-deal-with-cybersecurity/

[48] Ellen Nakashima, «U.S., Russia Agree to Set Up Computer Security Link.» Washington Post, 18 June 2013. Pg 10.

[49] For a news report on the sharp exchange between U.S. and Chinese officials over cyber espionage at the IISS Shangri-La Dialogue in Singapore (1 June 2013), see Ernesto Londono, "Hagel chides China for cyberspying, which draws rebuke from a general," Washington Post, 2 June 2013. Pg A15.

Assisting Other Nations in Strengthening Their Cyber Security Posture

A consistent policy theme being carried forward from the U.S. International Strategy for Cyberspace is to assist other nations in developing awareness of and strengthening their response to cyber threats, especially those that might emanate from within their own borders.[50] Assistance can include advice on protecting networks, educating and certifying cyber security professionals, standing up initial Computer Emergency Readiness Teams (CERTs), and organizing capacity within network operation centers and secure data centers.

Work is ongoing with the Government of the Islamic Republic of Afghanistan in many of these areas by the Departments of Commerce and Defense, as well as private universities and businesses.[51] U.S. is also assisting NATO partners bilaterally, as well as other developing countries around the globe who have expressed interest in working with the United States to improve their national cyber security posture. The logic of this engagement is simple: any place on the Internet that remains unsecured against malware is a potential vector into the Internet that could be a risk to all who use it. Hence, the more global the security the safer the Internet is for all.

Creating a Future Workforce Educated in Cyber Security

Another key aspect of U.S. cyber security is the education of a future general population that will be astute in on line security. This is part of a Department of Homeland Security program called «Stop-Think-Connect.» The United States is also educating a substantial cohort of highly skilled future cyber security professionals for service in both the private and public sectors. This pool of talent will serve to confront future challenges to the reliability, security and resiliency of the Internet, and protect the information that transits its infrastructure.

A key education initiative of the National Science Foundation is the Cyber Watch program, which began in 2005 as a consortium of 10 institutions in the Washington D.C. area. Today it is a nationwide program covering 29 states and consisting of 50 community colleges and 45 universities offering degrees and technical as well as non-technical cyber competitions. More than 40 businesses, government organizations and associations are affiliated with this program, which has also trained over 500 faculty members at its member institutions. Cyber Watch has developed several model Information Assurance Curricula for academic degrees and certifications in cyber security at every collegiate level.

---

[50] International Strategy for Cyberspace, May 2011. Pg 15 (Building Cyber Security capacity).

[51] Support for Afghanistan has been guided since 2004 mainly by the Defense Department's Telecommunications Advisory Team at ISAF.

More recently Cyber Watch has begun to extend its education to the high school level. Cyber Watch is one of the most promising educational programs for a future U.S. workforce of highly talented cyber security professionals.[52]

Another very important educational program is the National Security Agency's program for universities and colleges to be awarded the status of National Center of Academic Excellence in Information Assurance (i.e., cyber security) education. This program includes strict criteria for designations as either a Center of Academic Excellence for two year education programs, four year degree programs or as a Center of Excellence in information assurance research. As of 2013, 166 colleges have been awarded Center of Academic Excellence status in at least one category.[53]

Part II. NATO and Cyber Defense – 2013 Update[54]

Cyber Security first seized NATO attention at the head of states level in 2002, shortly after the Alliance suffered its first cyber attack. Since, cyber defense has rarely left the agenda of NATO's leadership or the agendas of leaders of its member states. These leaders have concluded that cyber attacks could reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability. In turn, Alliance agencies, commands, schools and staffs are working to realize the goals of preventing, detecting, defending against and recovering from any and all cyber attacks. Indeed, over the past 12 years cyber defense has become highly institutionalized across the Alliance and within its processes, including the core NATO Defense Planning Process.

The North Atlantic Treaty Organization (NATO) continues in 2013 to strengthen its capacity to defend its internal networks from a mounting number of daily intrusions, the threat of inadvertent compromise from user missteps, and from a steady stream of external cyber attacks. In early June Alliance Defense Ministers held their first ever meeting dedicated solely to cyber defense, a testimonial to the intensifying concern across NATO and among its members. It was agreed that as a priority defensive protection must be extended to all NATO owned and operated networks before the end of 2013. The ministers also tasked NATO staffs to provide a report by October on how NATO can support members who request assistance if they come under cyber attack.[55]

---

[52] See http://www.cyberwatchcenter.org/index.php?option=com_content&view=article&id=50&Itemid=29.

[53] See http://www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml.

[54] For further elaboration on this brief summary see the ACT website at http://www.act.nato.int/.

[55] See http://www.nato.int/cps/en/natolive/news_101143.htm. This is a news summary of the first day of the 4-5 June 2013 meeting of NATO defense ministers.

NATO's core interest in the cyber domain is the protection of Alliance owned and operated networks. As an alliance, NATO views the broader matter of cyber security as a national and not a NATO task. The Alliance does not want members to become dependent on NATO capabilities and thus reduce their national investments in cyber security. Although its focus is mainly on cyber defense, as the news report above indicates, the Alliance is studying whether or not it might be able to assist members who request help in responding to cyber attacks. To quote NATO Secretary General Anders Rasmussen, "Cyber attacks do not stop at national borders. Our defenses should not, either."[56]

Effective NATO Cyber Defense Governance

Cyber Defense is directed by the North Atlantic Council (NAC), as are all Alliance undertakings. In 2011, the NAC carried out the decisions of Alliance members at their summit at Lisbon in 2010. Those decisions called for a new cyber defense concept, policy and action plan – all of which the NAC approved by June 2011.

As a major enterprise, cyber defense oversight involves all NATO stakeholders, who meet together as the Cyber Defense Management Board. Day to day activities and management of programs is the business of the International Staff, in particular, the Cyber Defense Office within the Emerging Security Challenges Directorate. Another key staff is the NATO Headquarters Consultation, Command and Control Staff. This is a combined staff, comprised of members of the International Staff (primarily civilian) and International Military Staff (primarily military). This staff oversees cyber defense at NATO headquarters and agencies.

The NATO Communications and Information Agency (NCIA) directs the technical execution of cyber defense (among many other responsibilities). One element of NCIA is the NATO Computer Incident Response Capability (NCIRC), which is NATO's equivalent of a CERT – the primary monitor of networks for detecting and responding to intrusions and other risks to full operational capabilities.

The two NATO strategic commands play key roles in NATO cyber defense. Allied Command Operations (ACO) is responsible for command over all operational forces and therefore operates most of the networks that must be protected. Allied Command Transformation (ACT) has responsibility for the majority of cyber defense action plan items. Several action plan initiatives are discussed in more detail below.

NATO member nations, as already stated, have primary responsibility for their own cyber security. However where NATO and national networks interface the Alliance

[56] Ibid.

works with its members to ensure nations follow NATO's technical and procedural standards with regard to the protection of NATO information and classifications.

The Role of Allied Command Transformation

ACT is NATO's agent for change; its intellectual capital for the future. It is the command responsible for the multinational aspects of force transformation, which primarily is carried out by nations yet informed by NATO with respect to requirements for multinational interoperability. This role applies to cyber defense as it does to all NATO missions and functions. Thus ACT oversees a number of tasks aimed at strengthening NATO's cyber defense posture, both today and in the long term. The primary tasks of ACT are the development of Alliance (i.e., multinational) concepts and doctrine, and development of NATO training, education and exercises. All these apply to cyber defense just as they do to other military disciplines.

An additional important task is guiding development of NATO cyber defense capabilities of the future. This starts with fulfilling all the requirements already agreed but yet to be fully put in place. ACT also oversees planning for the longer term cyber defense requirements in order to stay abreast of anticipated future threats within expected resources. In developing future needs, Act takes into account operational lessons learned and assesses the effectiveness of current capabilities.

ACT has responsibility for developing NATO concepts and doctrine for cyber defense awareness, education and training for Alliance schools and for disseminating to members for use in their schools as appropriate. In 2013 NATO is on track to complete its update of cyber defense concepts and doctrine, and along with other staffs, ACT is guiding development of Alliance cyber defense training plans, education programs and exercises. Once completed, these products are to be reviewed by HQ NATO and nations. Like all training, cyber defense training proposals will ultimately be submitted to NATO's Military Committee for approval.

ACT is responsible for outreach programs to tap the expertise of industry and academia in seeking solutions to the many NATO cyber defense challenges. NATO has a well-developed regime for engaging with industry and this must now include cyber defense technologies. NATO is developing ties to academia through ACT to help Alliance staffs find innovative solutions to issues such as applying the concept of burden sharing to cyber defense, or determining NATO dependencies on national communication and information systems.

The Cooperative Cyber Defense Center of Excellence[57]

The CCD COE in Tallinn, Estonia has just celebrated its 5th anniversary and continues to strengthen its capacity in terms of resources and activities. 11 NATO members are sponsoring nations and two more have announced plans to join the Center's sponsors.[58] Although not a formal part of NATO's structure, CCD COE is an important and integral component of NATO's cyber defense team. ACT oversees all centers of excellence in terms of accrediting them with the Alliance and proposing inputs to their program of work. At present, the 2014 program of work for CCD COE is being prepared.

The CCD COE mission is to enhance capabilities, cooperation and information sharing across NATO, and among NATO nations and partners in cyber defense through education, research and development, lessons learned and consultation. The Center's goal is to be the main source of expertise in the field of cooperative cyber defense by accumulating, creating, and disseminating knowledge in related matters within NATO, NATO nations and partners. The three competency areas in which CCD COE pursues its goal are: legal and policy matters; training and doctrine issues; and research and development.

CCD COE has an impressive annual work plan of research publications, technical courses, conferences and cyber exercises. For example, in 2013 it has already completed its First Quarter 2013 Cyber Security Status Watch report; conducted its annual network defense exercise Locked Shield 2013 (in April), and its annual CyCon conference (in June).

Conclusions

There has been a marked increase in high profile disruptions of government and commercial enterprise networks over the past 18-36 months. These attacks suggest an increasing attraction of the cyber domain as the medium of choice for conducting attacks in pursuit of social and political as well as criminal motivations. We can expect this trend to continue and grow so long as the international community remains diffused on what constitutes acceptable behavior in cyberspace. Attackers may be criminals, or either state or non-state actors. While attribution remains difficult, the theory that any attacker has to expect some gain from conducting an

[57] See CCD COE website at https://www.ccdcoe.org/3.html.

[58] Centers of Excellence, being outside NATO are staffed and funded by sponsoring NATO members. The 11 members participating in CCD COE are Estonia, Germany, Hungary, Italy, Latvia, Lithuania, Netherlands, Poland, Slovak Republic, Spain and the United States. France, Turkey, and the UK have also announced plans to become sponsoring nations.

attack offers some indication of the source of attacks. Strengthening defenses is much more in the hands of legitimate network users, be they individuals, businesses or governments. All should raise their level of defense.

The United States is moving forward on several paths to strengthen its defenses, with a somewhat heightened sense of urgency in light of recent attacks around the world. Te United States is moving to strengthen the defensive posture of all online activities, both public and private – government agencies, businesses, organizations, communities and individuals. In this regard, the Departments of Defense and Homeland Security will ensure especially the security of the .mil and .gov domains. Overall, special attention is being given to the protection of critical infrastructure. A U.S. goal is a future population that is much more aware of risk even as it will be much more online. The United States is engaged internationally at all relevant junctures in the pursuit of a stronger framework of laws and norms to guide the legitimate use of cyberspace. Finally, the United States is interested in a culture of international cooperation to keep the Internet open and secure.

NATO is organized and is implementing a comprehensive program of cyber defenses that will protect its own networks. As an Alliance of 28 countries, NATO is establishing effective network governance and strong network defenses. What NATO has accomplished already in terms of organization, agreements and deployed defensive technologies is informative on what might eventually be achieved by the community of nations across the globe.

Disclaimer.

Dr. Charles Barry is an independent consultant and research fellow at the National Defense University. Views expressed in this paper are his alone and do not necessarily reflect the policies of the National Defense University, the Department of Defense or the United States Government.

Докладчик на Форуме
К.О.Песчаненко

Дылевский И.Н., Комов С.А.,
Песчаненко К.О., Петрунин А.Н.
Министерство обороны
Российской Федерации

О ПРИМЕНИМОСТИ НОРМ И ПРИНЦИПОВ МЕЖДУНАРОДНОГО ПРАВА К ВОЕННОЙ ДЕЯТЕЛЬНОСТИ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

В последнее время западное экспертное сообщество большое внимание стало уделять вопросу применимости существующих норм и принципов международного права к государственной деятельности в информационном пространстве. Толчком к этому послужило принятие американской Международной стратегии для киберпространства[59] (2011), в которой содержится утверждение о том, что существующие нормы и принципы международного права целиком и полностью применимы к деятельности государств в киберпространстве.

В сентябре 2012 юрисконсульт Государственного департамента США Гарольд Кох (Harold Honhgu Koh) выступил на конференции американского киберкомандования с докладом об американских подходах к тому, как международное право, по мысли автора, применяется к киберпространству[60]. Очевидно, что именно эти идеи нашли развитие в коллективном труде международной группы экспертов – «Таллинском руководстве о применимости

[59] The White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World 9 (2011), available at http://www.whitehouse.gov/sites/defarft/ffles/rss_viewer/ international_strategy_for_cybers pace.pdf

[60] Harold Honhgu Koh, Legal Advisor of the Dep't of State, International Law in Cyberspace, Address to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), available at http://www.state.gOV/s/l/releases/remarks/197924.htm.

международного права к кибервойне», подготовленном и опубликованном Центром кибероборонь НАТО на его сайте в начале 2013 года.[61]

Следует отметить, что российские эксперты в области военного использования информационно-коммуникационных технологий (ИКТ) с начала нынешнего века работают над определением возможностей распространения существующих норм и принципов международного права на военную деятельность в информационном пространстве[62]. Итогом этой работы стали «Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве» (2011), переданные в рамках обмена так называемыми «Белыми книгами» по дипломатическим каналам в США. В них дана российская трактовка применимости существующего международного права к военной деятельности в информационном пространстве[63]. В этом же году увидела свет «Конвенция об обеспечении международной информационной безопасности (концепция)»[64], в которую также вошли нормы и принципы регулирования военной деятельности государств в информационном пространстве. На международном уровне первой такой попыткой стало внесение от имени Шанхайской организации сотрудничества в 2011 году в Генассамблею ООН в качестве официального документа «Правила поведения в области обеспечения международной информационной безопасности»[65].

---

[61] Tallinn Manual on the International Law Applicable то Cyber Warfare (Michael N. Schmitt, gen. ed., forthcoming Cambridge University Press 2013), http://www.ccdcoe.org/249.html.

[62] S.A.Komov, S.V.Korotkov, S.N.Rodionov International Information Security: Military Aspects. Military Thought, volume 12, number 4, 2003, p.1-5

I.N.Dylevsky, S.A.Komov, S.V.Korotkov Military Aspects of Ensuring International Information Security in the Context of Elaborating Universally Acknowledged Principles of International Law. Disarmament Forum, **ICTS and International Security, number 3, 2007, p.35-43;**

S.M.Boyko, I.N.Dylevsky, S.A.Komov, S.V.Korotkov, S.N.Rodionov On International Legal Qualifications of Information Operations. Military Thought, volume 17, number 1, 2008, p.15-25;

International Information Security: Problems And Decisions, Shapter 3, Military-Political Aspects For Provision of International Information Security, Edited by Komov S.A., Moscow, 2011.

[63] Russian Federation Armed Forces' Information Space Activities Concept. Ministry of Defense of the Russian Federation. http://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle

[64] Convention on International Information Security (Concept), Moscow, 2011. http://www.mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/ 6912ce 36aa5f1e92c32579250035bebd!OpenDocument

[65] International Code of Conduct for Information Security. A/66/359. United Nations, General Assembly, 2011.

В рамках данного выступления представляется целесообразным пояснить российские подходы на примере принципиальных вопросов, поставленных в статье известного специалиста в области международного права, руководителя рабочей группы по разработке Таллинского руководства профессора М.Шмидта (Michael N. Schmitt),[66] посвященной сравнительному анализу подходов к проблеме применимости норм и принципов международного права к киберпространству американских и натовских экспертов.

Заранее приносим извинения за возможные неточности перевода и авторских интерпретаций. Итак, перейдем к перечню основных вопросов, поставленных в статье М.Шмидта.

1. Являются ли компьютерные атаки использованием силы и распространяется ли на них в этом случае запрещение такого использования по смыслу Статьи 2 (4) Устава ООН и общепринятого международного права?

В отношении вопроса применения силы в информационном пространстве необходимо отметить следующее. В резолюции Генеральной Ассамблеи ООН «Определение агрессии» №3314 (XXIX)[67] от 14 декабря 1974 года дано общее определение агрессии (ст. 1), указан основной критерий квалификации агрессивного акта (ст. 2), перечислены основные акты агрессии (ст. 3), указывается, что их перечень не является исчерпывающим и Совет Безопасности может определить, что другие акты представляют собой агрессию согласно положениям Устава ООН (ст.4). Например, таким актом может стать компьютерная или электромагнитная атака на объекты информационной инфраструктуры критически важных объектов, от функционирования которых напрямую зависит национальная и международная безопасность.

Вследствие того, что США в свое время не признали данную резолюцию, использовать ее потенциал на практике пока не представляется возможным. А вместе с тем, такой термин как **«киберагрессия»** (cyber-aggression) закреплен в Национальной военной стратегии США (2011)[68].

Сейчас принцип запрещения применения силы или угрозы силой в отношении территориальной целостности или политической независимости

[66] Michael N. Schmitt, International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed, Harvard International Law Journal, Volume 54, December 2012, pp.13-37, http://www.usnwc.edu/Academics/Faculty/Michael-Schmitt.aspx

[67] 3314 (XXIX). Definition of Aggression, 2319th plenary meeting, 14 December 1974. http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/739/16/IMG/NR073916.pdf? OpenElement

[68] The National Military Strategy of the United States of America, Redefining America's Military Leadership, 2011, p.15

другого государства традиционно применяется только в отношении **физической силы**. Основываясь на документах и правоприменительной практике ООН, пока не представляется возможным однозначно ответить на вопрос о том, будет ли нападение в рамках информационной атаки или операции признано агрессией, применением силы или угрозы силой. Это свидетельствует о необходимости содержательного развития данных терминов, направленного на четкое определение этих понятий. В этой связи хотелось бы отметить, что целесообразно включить данный вопрос в повестку дня Совета Безопасности ООН и принять общепризнанное обязывающее международно-правовое определение «агрессии» в его широком смысле, включающем, в том числе, информационную агрессию и другие подвиды этого противоправного деяния.

2. Может ли быть использовано право государств на самооборону и коллективную оборону, признанное в Статье 51 Устава ООН, в ответ на информационные атаки, которые составляют вооруженное нападение?

В данном вопросе усматривается аналогия с предыдущим вопросом. В этом случае, в свою очередь, необходимо определиться с понятиями «вооруженное нападение» в форме информационной атаки. Не решив эту проблему в рамках ООН, нельзя говорить о возможности применения этой нормы. Кроме того, необходимо разработать оперативно-технические методы достоверного установления источников враждебных информационных атак.

Пока эти проблемы не решены, нет полной ясности относительно того, имеется ли основа для проведения ответных военных действий против государств, проводящих информационные атаки. Поэтому если определенные виды таких атак будут квалифицированы ООН как вооруженное нападение, пострадавшая сторона будет иметь законное право на самооборону. Однако в этом случае должен быть решен вопрос о характере симметричного или несимметричного ответа (с использованием обычного вооружения). В этой связи следует отметить, что принятие НАТО решения провести такую квалификацию в рамках альянса имеет правоприменительную сферу, ограниченную только членами Вашингтонского договора. Правовым же путем решения данной проблемы в глобальном масштабе на сегодняшний день остается только принятие соответствующего международно-правового акта ООН. Так как сейчас подобного документа не существует, то может быть использовано обращение за помощью в Совет Безопасности ООН с тем, чтобы он квалифицировал информационную атаку как угрозу миру или агрессию и предпринял определенные меры, предусмотренные Уставом ООН.

3. Должны ли государства, проводящие военные действия в информационном пространстве, принимать во внимание суверенитет других государств, в том числе и в мирное время?

На этот вопрос российская сторона дает положительный ответ без всяких оговорок. Информационное пространство глобально, однако информационные структуры, создающие его, находятся на национальных территориях и имеют конкретную национальную принадлежность. Конечно, не исключается то, что на территории одного государства будут размещены информационные системы других государств или даже находящиеся под международным управлением. Вместе с тем, вопрос определения национальной принадлежности каждой информационной системы не представляет неразрешимой проблемы и вполне может быть решен в рамках существующих правовых процедур.

В этой связи следует отметить, что ст.32 в) Конвенции СЕ о киберпреступности (2001)[69] своими положениями нарушает общепризнанные принципы уважения государственного суверенитета и невмешательства во внутренние дела других государств, допуская проведение оперативно-розыскных мероприятий в зарубежных компьютерных сетях без уведомления обЦ этом национальных властей.

Есть еще одно важное обстоятельство, которое российская сторона воспринимает как вмешательство во внутренние дела других государств. Оно касается трансграничных информационно-психологических воздействий, для реализации которых, как правило, используются электронные СМИ. Полагаем, что этот вопрос может быть решен уже сейчас на основе положений, содержащихся в Декларации принципов международного права, а также в Декларации о недопустимости вмешательства во внутренние дела государств, об ограждении их независимости и суверенитета: «Никакое государство не имеет права вмешиваться прямо или косвенно по какой бы то ни было причине во внутренние и внешние дела другого государства. Вследствие этого осуждаются не только вооруженное вмешательство, но также все другие формы вмешательства и всякие угрозы, направленные против правосубъектности государства или против его политических, экономических и культурных элементов». [70]

---

[69] Convention on Cybercrime (ETS № 185), Council of Europe (2001). http://conventions.coe.int/Treaty/Commun/ ChercheSig.asp? NT=185&CM=8&DF =&CL=ENG

[70] 2131 (XX). Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty 1408th plenary meeting, 21 December 1965. http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/218/94/IMG/NR021894.pdf? OpenElement

Несмотря на то, что в этих документах не дается четкого определения понятия «вмешательство во внутренние дела государств», в них приведен перечень действий, составляющих такое вмешательство.

В последующем угроза вмешательства во внутренние дела государств была раскрыта более детально в Декларации о недопустимости интервенции и вмешательства во внутренние дела государств[71], принятой в 1981 г. на 36-ой сессии ГА ООН, через институты прав и обязанностей государства. В этом международно-правовом акте информационная составляющая угрозы включила:

- вмешательства в систему информации и средств массовой информации;
- любые клеветнические кампании, оскорбительная или враждебная пропаганда с целью осуществления интервенции или вмешательства во внутренние дела других государств;
- распространение фальшивых или искаженных сообщений, которые могут рассматриваться как вмешательство во внутренние дела других государств или как наносящие ущерб укреплению мира, сотрудничества и дружественных отношений между государствами и нациями.

Опираясь на данную правовую основу, можно сделать вывод, что практически любая информационная операция психологической направленности, проводимая в мирное время в отношении другого государства, будет обладать признаками вмешательства в его внутренние дела. Это касается, в том числе, вопросов «продвижения демократии», которые не могут служить оправданием проведения подобных акций.

4. Применимо ли гуманитарное право к информационным атакам?

Производными от этого общего вопроса следует считать и ряд следующих частных вопросов, поставленных М.Шмидтом, т.к. все они относятся к сфере гуманитарного права:

4.1. Следует ли придерживаться принципа пропорциональности при проведении информационных атак?

4.2. Должен ли атакующий различать военные и невоенные цели и как в этой связи быть с инфраструктурой двойного назначения?

4.3. Нужно ли анализировать различные типы информационного оружия с точки зрения их соответствия нормам и принципам гуманитарного права?

[71] 36/103. Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States, 91st plenary meeting, 9 December 1981. http://daccess-dds-ny.un.org/doc/RESOLUTION/ GEN/NR0/407/29/IMG/NR040729.pdf?OpenElement

4.4. Отвечают ли государства за действия в информационном пространстве уполномоченных ими лиц?

В преамбуле «Конвенции о запрещении или ограничении применения конкретных видов обычного оружия, которые могут считаться наносящими чрезмерные повреждения или имеющими неизбирательное действие» (1981 г.) записано, что «право сторон в вооруженном конфликте выбирать методы и средства ведения войны не является неограниченным». Детально данный принцип раскрывается в «основных нормах», характеризующих допустимые методы и средства ведения войны, сформулированных в ст. 35 первого Дополнительного протокола 1977 г. к Женевским конвенциям от 12 августа 1949 г. о защите жертв войны[72]. Там прямо указано, что запрещается применять оружие и методы ведения военных действий, способные причинить излишние повреждения или излишние страдания.

Отсюда следует, что можно информационные атаки квалифицировать исходя из масштаба и тяжести их последствий. Так, дезорганизация функционирования финансовой системы государства, техногенные катастрофы и паника, вызванные проведением информационных атак, могут привести к массовым жертвам среди мирного населения. Следовательно, в соответствии с международным гуманитарным правом и принципом пропорциональности должен налагаться запрет на проведение подобных акций.

Кроме того, в международных конвенциях сложилось правило запрещения или ограничения тех видов оружия, которые имеют неизбирательное действие, т.е. в равной мере опасны как для военных, так и для гражданских объектов[73].

Поэтому нельзя применять информационное оружие, которое действует неизбирательно, т.е. как против военных, так и против гражданских объектов, причиняет излишние повреждения и страдания. Решение вопроса об атаках на объекты двойного назначения требует определения степени их вклада в эффективность военных действий. В том случае, если эта степень достаточно велика, объект двойного назначения может быть признан военным, со всеми вытекающими последствиями. Однако в этом случае, не должен нарушаться принцип пропорциональности, т.е. не должен наноситься неприемлемый ущерб гражданской инфраструктуре. Все это требует разработки соответствующей методологии и внедрения ее в практику оперативной и боевой подготовки войск.

---

[72] Additional Protocol I to the Geneva Conventions (adopted on August 12, 1949), Article 35.

[73] Additional Protocol I to the Geneva Conventions (adopted on August 12, 1949), Article 52, par. 2; Article 57.

[74] Additional Protocol I to the Geneva Conventions (adopted on August 12, 1949), Article 36.

В соответствии со ст.36 Дополнительного протокола 1[74] при изучении, разработке, приобретении или принятии на вооружение новых видов оружия, в том числе информационного оружия, средств или методов его применения следует определить, подпадает ли их применение, при некоторых или при всех обстоятельствах, под ранее названные запрещения. При этом такой анализ должен быть ориентирован, в первую очередь, на выявление их способности наносить чрезмерные повреждения или осуществлять неизбирательные действия. Такие виды информационного оружия должны быть запрещены. Вместе с тем, сегодня нет не только методик проведения такого анализа, не существует даже общепринятой классификации информационного оружия.

Вопрос об ответственности государства за действия в информационном пространстве уполномоченных ими лиц затрагивает значительно более широкую проблему участников вооруженного конфликта с использованием информационного оружия. Нормы современного международного права устанавливают, что война должна вестись только между вооруженными силами соответствующих государств (комбатантами)[75]. Причем в состав вооруженных сил (регулярных и нерегулярных) входят силы милиции (полиции), безопасности, добровольческие отряды, отряды ополчения, партизаны, а также население, которое по собственному почину берется за оружие для борьбы с вторгающимися войсками, не успев сформироваться в регулярные части. Все указанные категории сражающихся рассматриваются в качестве законных участников войны, если они удовлетворяют следующим условиям, предусмотренным конвенциями:

- имеют во главе лицо, ответственное за своих подчиненных;

- имеют определенный и ясно видимый издали отличительный знак;

- открыто носят оружие;

- соблюдают в своих действиях законы и обычаи войны.

Очевидно, что некоторые из перечисленных пунктов не только не согласуются со спецификой проведения трансграничных информационных атак, но и не могут быть напрямую внедрены в практику расследования фактов их проведения. Таким образом, определение статуса «комбатанта» применительно к действующим в информационном пространстве лицам также требует разработки и внедрения соответствующей международно-правовой методологии. В противном случае задача привлечения к от-

[75] Additional Protocol I to the Geneva Conventions (adopted on August 12, 1949), Article 43.

ветственности конкретных государств и соответствующих должностных лиц представляется неразрешимой.

Теперь, наконец, попытаемся дать ответ на обобщающий вопрос, поставленный М.Шмидтом: **«Могут ли имеющиеся в настоящее время общепризнанные принципы международного права быть применены к военной деятельности в информационном пространстве»**?

Всеобъемлющий ответ на него основывается на всех предыдущих рассуждениях и, соответственно, не является однозначно положительным. Совершенно ясно, что только часть существующих норм и принципов международного права может быть распространена на военную деятельность в информационном пространстве. Однако даже этот шаг потребует разработки процессуальных норм или специальной международно-правовой методологии, а также выполнения ряда важных условий как организационно-правового, так и технологического характера.

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

THE APPLICABILITY OF THE NORMS AND PRINCIPLES OF INTERNATIONAL LAW TO THE MILITARY ACTIVITIES IN CYBERSPACE

Over the last few years Western experts began to pay a much closer attention to the problem of applicability of existing norms and principles of international law to the activities of the government in the information domain. Such a close scrutiny by the expert community followed the adoption of *The Strategy for Cyberspace*[76] (2011) proposed by the USA which states that the existing norms and principles of international law are fully applicable to activities of governments in cyberspace.

In September 2012 Harold Honhgu Koh, Legal Advisor of the Department of State addressed the USCYBERCOM Inter–Agency Legal Conference with a report describing the American view on the application of the international law to cyberspace[77]. The same ideas were apparently further promoted in the work of the international group of experts which resulted in *The Tallinn Manual on the International Law Applicable to Cyber Warfare* prepared and published by the NATO Cooperative Cyber Defense Centre of Excellence at its official webpage in early 2013.[78]

It is worthwhile to point out that Russian experts in military use of information and communication technologies (ICTs) have been since the turn of the century studying the possibility of extrapolating the existing norms and principles of international law onto cyber warfare[79]. As a result of this work the document titled *The Russian Federation Armed Forces' Information Space Activities Concept* (2011) was handed over through diplomatic channels to the United States of America as part

[76] The White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World 9 (2011), available at http://www.whitehouse.gov/sites/defarft/ffles/rss_viewer/ international_strategy_for_cybers pace.pdf

[77] Harold Honhgu Koh, Legal Advisor of the Dep't of State, International Law in Cyberspace, Address to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), available at http://www.state.gOV/s/l/releases/remarks/197924.htm.

[78] Tallinn Manual on the International Law Applicable то Cyber Warfare (Michael N. Schmitt, gen. ed., forthcoming Cambridge University Press 2013), http://www.ccdcoe.org/249.html.

[79] S.A.Komov, S.V.Korotkov, S.N.Rodionov International Information Security: Military Aspects. Military Thought, volume 12, number 4, 2003, p.1-5

of the so-called exchange of White Books. The above document offers the Russian view on the problem of applicability of the existing norms of international law to military activities in the information space[80]. The same year another document was developed with the title *The Convention on International Information Security (Concept)*[81] which also describes the norms and principles of legal regulation of military activity of nations in cyberspace. The first international initiative in the area was the official document titled *International Code of Conduct for Information Security*[82], developed and submitted by the Shanghai Cooperation Organization to the UN General Assembly in 2011.

It shall be appropriate to take a moment to clarify the Russian view as exemplified by the major problems raised by Michael N. Schmitt a renowned expert in the field of international law and the head of the group of experts who developed The Tallin Manual in his article on the comparative analysis of the approaches to the problem of applicability of norms and principles of international law to cyberspace exercised by U.S. and NATO experts[83].

We would like to apologize in advance for any unintentional errors through translation and our interpretation of the source text. Let us now turn our attention to the list of major problems raised by Michael N. Schmitt in his article.

1. Can cyber-attacks be classified as a use of force and shall they be prohibited through Article 2(4) of the UN Charter and generally accepted principles of international law?

When considering the problem of the use of force in cyberspace, the following should be noted: the UN General Assembly resolution No. 3314 (XXIX) Definition of Aggression[84], of 14 December 1974 sets forth the general definition of aggression (Article 1), specifies the principal criterion qualifying an act of aggression (Article 2), lists all major acts of aggression (Article 3), indicates that the provided list is not exhaustive and subject to a decision of the Security Council other acts may be

[81] Convention on International Information Security (Concept), Moscow, 2011. http://www.mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/ 6912ce 36aa5f1e92c32579250035bebd!OpenDocument

[82] International Code of Conduct for Information Security. A/66/359. United Nations, General Assembly, 2011.

[83] Michael N. Schmitt, International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed, Harvard International Law Journal, Volume 54, December 2012, pp.13-37, http://www.usnwc.edu/Academics/Faculty/Michael-Schmitt.aspx

[84] 3314 (XXIX). Definition of Aggression, 2319th plenary meeting, 14 December 1974. http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/739/16/IMG/NR073916.pdf? OpenElement

qualified as aggressive under the provisions of the United Nations Charter (Article 4). For instance, a cyber or electromagnetic attack on critical elements of the information infrastructure which are directly engaged in maintaining national and international security may be qualified as an act of aggression.

The United States have not subscribed to the above resolution, therefore its practical application is not yet possible. And at the same time, the U.S. National Military Strategy (2011) recognized the term "**cyber-aggression**"[85].

Presently the prohibitive principle of use of force or threat of force against territorial integrity or political independence of another state traditionally refers only to **physical force**. Taking into consideration the documents and legal practice of the UN it is not yet possible to state explicitly whether a cyber-attack or cyber-operation shall be recognized as aggression, use of force or threat of force. This demonstrates the urgent need for a clear legal definition for the above concepts. We, therefore, we would like to recommend to include this problem into the UN Security Council agenda to adopt a legal definition for "aggression" that would be globally accepted and binding in its broadest sense, including, inter alia, the instances of cyber-aggression and its other subtypes.

2. May a nation use its right for self-defense and collective defense referred to in Article 51 of the United Nations Charter in response to cyber-attacks which constitute an armed attack?

This question is rather analogous to the previous problem. The term «armed attack in the form of cyber-attack» requires a clear legal definition. Without solving this legal problem at the UN level one can envision no practical applications. Furthermore, technical means for urgent and reliable identification of sources of hostile cyber-attacks must be found.

As long as these problems remain unresolved, there is no clear understanding whether a nation has a right to military retaliation against states initiating cyber-attacks. When certain types of such attacks are qualified by the United Nations as armed attacks the victim thereof shall have a lawful right to self-defense. This, however, raises the issue of the nature of a symmetric or asymmetric retaliation (using conventional warfare). In this regard it is worthwhile to note that the adoption by NATO of an internal qualification shall have a legal effect only between the members to the Washington Treaty. Today, the only global legal solution to the problem is adoption of a corresponding international instrument by the UN.

[85] The National Military Strategy of the United States of America, Redefining America's Military Leadership, 2011, p.15

Since a document like that yet remains to be passed a nation may appeal to the UN Security Council to qualify a cyber-attack in question as posing threat to peace or being an act of aggression to take necessary action reserved by the UN Charter.

3. Should nations conducting military operations in cyberspace observe the sovereignty of other nations including in times of peace?

The Russian side gives an affirmative answer to this question without reservations. Although the information space itself is global in nature, the physical elements of the information infrastructure are located in national territories and therefore have a specific national identity. Having said that, we must recognize the fact that a nation may accommodate foreign or even international information systems. Determining a national identity of each such information system does not, however, pose an unsolvable problem and can be resolved through applicable legal proceedings.

Likewise, it is worthwhile to note that Article 32 of *The Convention on Cybercrime adopted* by the Council of Europe (2001)[86] goes against the generally recognized principles of respect for national sovereignty and non-interference in the internal affairs of other nations by endorsing investigations affecting foreign computer networks without notifying the government of such nation.

There is yet another important aspect that the Russian side deems an interference in the internal affairs of other nations which relates to cross-border psychological information impacts which are, as a rule, conducted through the agency of electronic media. We are of an opinion that this issue can be resolved today based on the provisions of *The Declaration of Principles of International Law and The Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty* which specifically states that "No State has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are condemned.»[87]

Despite the fact that the above documents do not give a clear definition of the term «interference in the internal affairs of states», they nonetheless provide a list of actions which constitute such interference.

[86] Convention on Cybercrime (ETS № 185), Council of Europe (2001). http://conventions.coe.int/Treaty/Commun/ ChercheSig.asp? NT=185&CM=8&DF =&CL=ENG

[87] 2131 (XX). Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty 1408th plenary meeting, 21 December 1965.

Later on the threat of intervention in the internal affairs of states was determined in more detail in *The Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States*[88] adopted in 1981 at the 36th session of the UN General Assembly through the institutions of rights and obligations of states. The above international legal instrument defines the information component of a threat as follows:

- intervention in the information system and the media;
- any smear campaigns, abusive or hostile propaganda aiming to intervene or interfere in the internal affairs of other states;
- dissemination of false or distorted information which can be considered as interference in the internal affairs of other states or impediment to peace-keeping efforts, cooperation or friendly relations between states and peoples.

Considering the above legal definition it is possible to conclude that almost any information action involving a psychological impact conducted in peacetime against another state will have certain characteristics of interference in the internal affairs of such state. This applies, in particular, to the "democratization" projects that cannot justify any such action.

4. Shall the humanitarian law be applicable to information attacks?

This general question gives rise to a number of more specific questions posed by Michael Schmitt in relation to the humanitarian law:

4.1. Should the principle of proportionality be observed when conducting a cyber-attack?

4.2. Should the attacking party distinguish between military and non-military targets and how dual-purpose infrastructure should be treated?

4.3. Should different types of cyber warfare be analyzed in terms of their compliance with the norms and principles of the humanitarian law?

4.4. Should nations be responsible for the actions in information space taken by persons authorized thereby?

The preamble to *The Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects* (1981) states that "the right of the parties to an

[88] 36/103. Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States, 91st plenary meeting, 9 December 1981. http://daccess-dds-ny.un.org/doc/RESOLUTION/ GEN/NR0/407/29/IMG/NR040729.pdf?OpenElement

armed conflict to choose methods or means of warfare shall not be unlimited". This principle is revealed in detail in the "basic norms" describing the permissible means and methods of warfare set forth in Article 35 of the First Additional Protocol of 1977 to the Geneva Conventions of 12 August 1949 on the Protection of War Victims[89], which clearly states that weapons and methods of warfare that cause excessive damage and unnecessary suffering are prohibited.

It follows from the above that cyber-attacks can be classified based on the scale and severity of their impacts. For instance, disruption of a national financial system, anthropogenic accidents and panic caused by through cyber-attacks may cause massive casualties among the civilian population and therefore, under the international humanitarian law and the principle of proportionality must be prohibited.

Furthermore, active international conventions ban or restrict the use of weapons having indiscriminate effects as they pose an equal threat both to military and civilian objects[90].

Therefore, information weapons that have indiscriminative effects, i.e. target both military and civilian objects must not be used as they cause excessive damage and unnecessary suffering. While planning attacks on dual-purpose facilities the overall effect for the military campaign must be considered. When such effect is high enough, then such dual-purpose facility may be recognized as military-purpose and treated accordingly. However, the principle of proportionality must not be violated, i.e. no excessive damage to civilian infrastructure shall be allowed. Such approach will require development of appropriate methodology and its practical application in operational and combat training of troops.

In accordance with Article 36 of Additional Protocol I to the Geneva Conventions[91], the study, development, acquisition or making operational a new type of weapon, including information weapons and means or methods of its application, it must be considered whether the use of such weapon, in some or all circumstances, go against previously adopted prohibitions. Such analysis should be primarily focused on identifying capabilities to inflict excessive damage or produce indiscriminative effects. Any such types of information weapons must be banned. However, not only appropriate analytical methods yet remain to be developed, but there is yet no generally accepted classification for information weapons.

---

[89] Additional Protocol I to the Geneva Conventions (adopted on August 12, 1949), Article 35.

[90] Additional Protocol I to the Geneva Conventions (adopted on August 12, 1949), Article 52, par. 2; Article 57.

[91] Additional Protocol I to the Geneva Conventions (adopted on August 12, 1949), Article 36.

The issue of responsibility of the state for the activities of the state authorized persons in cyberspace touches upon a much deeper problem of the parties involved in an armed conflict with the use of information weapons. Currently the norms of the international law recognize that a war may be conducted only between the armed forces of the states in conflict (combatants)[92]. The armed forces (both regular and nonregular troops) includes the police force, security personnel, volunteers, militia, partisans and civilians who on their own accord choose to offer the invading enemy armed opposition who have not had time to form regular troops. All the above categories are considered to be legitimate combatants when they meet the following conditions set forth by adopted conventions:

- have a commander who bears responsibility for their actions;
- have a distinctive emblem clearly visible from a distance;
- openly carry arms;
- comply with the laws and traditions of waging a war.

It is obvious that some of the above items are not only inconsistent with the specifics of cross-border information attacks, but cannot have direct practical applications for investigating such attacks. In particular, the legal status of «combatant» as relates to people active in cyber-space requires a well-developed international legal methodology or otherwise the problem of bringing offending states and their officials to justice deems to have no solution.

Finally we shall try to answer the generalizing question put forth by Michael Schmitt: **«May the current generally recognized principles of international law be applicable to military operations in cyberspace?»**

A comprehensive answer to the above question is based on all the previous arguments and, consequently, may not be unequivocally positive. It is absolutely clear that only a certain part of the existing norms and principles of international law can be extended to military activities in the cyberspace. However, even where such extension is possible, it will require the development of procedural norms or a specialized international legal methodology, as well as a number of important conditions relating to organizational, legal, and technological issues.

[92] Additional Protocol I to the Geneva Conventions (adopted on August 12, 1949), Article 43.

Стрельцов А.А.
Институт проблем информационной безопасности
МГУ имени М.В.Ломоносова

ПРОБЛЕМЫ АДАПТАЦИИ МЕЖДУНАРОДНОГО ПРАВА К ИНФОРМАЦИОННЫМ КОНФЛИКТАМ

Информационные конфликты становятся реальностью. Как было отмечено в докладе, подготовленном Группой правительственных экспертов ООН по международной информационной безопасности и представленном Генеральным Секретарем ООН 65 сессии ГА ООН (2010 г.), «агрессивное» использование информационных и коммуникационных технологий составляет угрозу международному миру и безопасности.

Это предопределяет значительное внимание международного сообщества к проблемам регулирования общественных отношений, связанных с созданием условий для предупреждения, прекращения и ликвидацией последствий конфликтов между государствами в информационной сфере.

Основными источниками права в данной области являются Устав ООН, международные договоры, заключаемые в развитие положений Устава ООН по обеспечению международного мира и безопасности, международные договоры по гуманитарным аспектам ведения войны, решения Международного Суда, содержащие трактовки положений международного права использования силы.

Непосредственное применение норм международного права, содержащихся в данных источникам, во многом затруднено вследствие особенностей информационной сферы и, прежде всего, глобального информационного пространства как объекта права.

К числу таких особенностей относятся:

• не наблюдаемость невооруженным глазом (без использования специальных технологий) объектов «силового» воздействия – программных кодов и информационных массивов;

• не наблюдаемость средств «силового» воздействия и субъектов их использования;

• не наблюдаемость невооруженным глазом (неочевидность) причинно-следственной связи между возникающими негативными последствиями «силового» воздействия на процедуры выполнения компьютерных вычислений и коммуникационных операций;

• неопределенность методов оценки негативных последствий вредоносного применения информационных и коммуникационных технологий.

Вследствие этого теряет черты определенности как содержание правовых норм международного права, так и процедура фиксации юридических фактов, порождающих правоотношения, связанные с применением силы, угрозой применения силы, вооружённым нападением и другими событиями, составляющие предмет международного права в области вооруженных конфликтов.

В этих условиях применению норм международного права должна предшествовать их адаптация к терминам, объектам и субъектам информационной сферы, к специфике использования информационных и коммуникационных технологий в качестве так называемого «информационного оружия».

Можно выделить три основных направления адаптации международного права к информационным конфликтам.

Первое направление адаптации заключается в подготовке согласованной трактовки принципов поведения государств-членов ООН применительно к информационной сфере. Эти принципы можно было бы выразить в форме правил поведения государств в информационной сфере. Один из возможных подходов к выполнению данной задачи содержится в представленном Российской Федерацией совместно с Китаем, Таджикистаном и Узбекистаном Генеральному Секретарю ООН проекте Правил поведения в информационном пространстве. При подготовке данного документа учитывались правила поведения государств, закреплённые в Уставе ООН, положения резолюций Генеральной Ассамблеи ООН по вопросам «Достижения в сфере информатизации и коммуникаций в контексте международной безопасности» (1999-2010 гг.) и по созданию глобальной культуры кибербезопасности (2007-2009 гг.).

Второе направление адаптации охватывает вопросы формирования системы мер доверия между государствами в информационной сфере. До-

верие является исключительно важным условием предотвращения информационных конфликтов. Содержание и форма системы мер доверия требуют особого рассмотрения.

Третье направление адаптации международного права предполагает подготовку согласованной позиции государств-членов ООН по следующим основным аспектам:

содержания норм права в терминах информационной силы и информационной сферы и формы их закрепления;

содержания и формы закрепления процедурных норм фиксации юридических фактов и согласованной деятельности государств по проведению необходимых оперативно-следственных мероприятий;

функций, структуры и принципов функционирования международной системы мониторинга глобального информационного пространства;

визуализации объектов и субъектов, защищаемых международным гуманитарным правом.

При всей трудности подготовки и заключения международных договоров в области применения международного права к информационным конфликтам, представляется важным приступать к этой работе.

В условиях расширения исследований и накопления в зарубежных государствах практики использования информационных и коммуникационных технологий для «силового» разрешения межгосударственных противоречий одной из актуальных проблем становится анализ способов и методов применения международного права к информационным конфликтам.

Важность развития международного сотрудничества в данном направлении все более отчетливо осознается государствами – членами международного сообщества. Как известно, уже длительное время консенсусом принимаются выдвигаемые по инициативе Российской Федерации и некоторых других государств проекты резолюций Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности". Группа правительственных экспертов ООН по информационной безопасности (2009-2010 гг.), подготовившая проект доклада Генерального Секретаря ООН на 65 сессии Генеральной Ассамблеи ООН, включила в данный проект доклада рекомендацию «принять меры по … обеспечению стабильности и уменьшению рисков в связи с последствиями государственного использования информационных технологий».

Правовое обеспечение международной безопасности и сохранения мира базируется, прежде всего, на принципах и нормах международного права, закрепленных в Уставе ООН, Гаагских и Женевских конвенциях, решениях Международного Суда, многосторонних и двусторонних договорах, заключенных в области обеспечения безопасности.

Вряд ли подлежит сомнению, что эти принципы и нормы применимы и к ситуациям, связанным с нарушением международной безопасности и мира вследствие враждебного использования информационных технологий. В то же время, как представляется, в правовом регулировании отношений в рассматриваемой области существуют определенные пробелы.

Эти пробелы касаются, в первую очередь, следующих вопросов:

квалификации информационных технологий в качестве разновидности оружия и, соответственно, – атак на информационные системы критически важных объектов информационной инфраструктуры противостоящего государства с использованием информационных технологий – в качестве разновидности вооруженного нападения;

методов и способов визуализации (придания материального, объективного вида) атак, осуществляемых с использованием информационных технологий, их последствий, а также субъектов, реализующих такие атаки;

методов и способов обеспечения безопасности объектов информационной инфраструктуры, используемых лицами и организациями, защищаемыми международным гуманитарным правом, в том числе гражданским населением, пленными, ранеными и больными, Международным Красным Крестом, а также лицами и организациями, обеспечивающими сохранение культурных ценностей;

методов и способов обеспечения государственного нейтралитета в условиях враждебного использования государствами информационных технологий;

методов и способов подготовки и представления доказательств при обращении в Международный Суд с жалобами по фактам враждебного использования государствами информационных технологий для нарушения суверенитета, территориальной целостности и политической независимости.

Необходимо отметить, что право как механизм поддержания справедливости в отношениях конфликтующих сторон базируется, прежде всего, на презумпции наблюдаемости (возможность фиксирования субъектов с помощью органов чувств) и объективной документируемости (существование стороннего наблюдателя, способного представить свидетельские показания), на-

личия юридических фактов, порождающих, изменяющих или прекращающих правоотношения, обусловленные нормами соответствующего права.

В то же время киберпространство, в котором происходят акты применения «информационной силы», в том числе с использованием информационных и коммуникационных технологий, такими свойствами не обладает.

Устранение отмеченных пробелов в международном правовом регулировании общественных отношений в области предупреждения враждебного использования информационных технологий может быть осуществлено в рамках адаптации существующих норм права к современным реалиям.

К числу основных направлений адаптации международного права можно было бы отнести следующие:

адаптация правовых норм, закреплённых в источниках права;

адаптация системы фиксации юридических фактов, определяющих возникновение, изменение или прекращение правоотношений, связанных с применением силы или гуманитарной защиты определенных объектов и субъектов;

адаптация системы выявления субъекта агрессивного применения информационных и коммуникационных технологий;

визуализации объектов и субъектов, защищаемых нормами международного гуманитарного права.

К процессу адаптации естественно было бы предъявить требование обязательности для всех государств адаптированных норм прав и правовых процедур. В противном случае эти нормы и процедуры будут носить рекомендательный характер и не смогут восполнить пробелы в международном праве.

Процесс поиска механизмов адаптации международного права и подготовки предложений по содержанию адаптированных норм права, по существу, уже начался. Такого рода предложения, в частности, выдвинуты в 2011 г. Российской Федерацией совместно с некоторыми другими государствами в качестве официального документа ООН «Правила поведения государств в информационной сфере». Достаточно детальная проработка возможных адаптированных правовых норм, регулирующих отношения в области враждебного использования информационных технологий, осуществлена международной группой экспертов по заданию Совместного центра НАТО по обмену передовым опытом в сфере киберзащиты в Эстонии. Эти предложения известны под названием Таллиннское руководство по киберконфликтам.

Prof. Streltsov A.A.,
Institute of Information Security Issues,
Lomonosov Moscow State University

OPEN PROBLEMS OF INTERNATIONAL LAW ADAPTATION TO INFORMATION CONFLICTS

Information conflicts today are becoming a new reality. Quoting the report prepared by an UN Group of Governmental Experts in international information security and read by the UN Secretary General at the 65th session of the UN General Assembly in 2010 "aggressive" use of information and communication technologies poses a threat to international peace and security.

Thus, a significant degree of attention is given by the international community to the problem of regulating social relations in order to prevent, stop and eliminate adverse consequences of conflicts between nations in the information arena.

The main sources of the legal authority in the above area are represented by the United Nations Charter, international treaties concluded in pursuance of the provisions of the UN Charter to maintain international peace and security, international treaties concerning humanitarian aspects of war, decisions of the International Court of Justice offering interpretations of provisions of the international law allowing the use of force.

Direct application of the norms of international law contained in the sources referred to above is rather problematic due to the peculiar nature of the information domain and, above all, the role of the global cyberspace as an object of law.

Such peculiar characteristics include as follows:

- targeted objects, such as program codes and data arrays are unobservable with 'a naked eye' and require the use of special technologies
- Means and agents of targeting are unobservable;
- The cause-and-effect relationship between negative impacts onto computing and communication procedures and instances of applied «force» cannot be traced and are not evident without the use of special methods
- methods for assessing adverse effects of hostile use of information and communication technologies have not been explicitly developed.

Taking the above into account, both the existing legal norms of the international law and the procedure of ascertaining legal facts that give rise to legal relations

relating to the use of force, threat of force, an armed attack, or other such events that constitute the subject matter of international law in armed conflicts become rather vague and ambiguous.

Therefore application of norms of international law must be preceded by adaptation of the same to the specific terms, objects and subjects of the information domain and the peculiarities of information and communication technologies used as the so-called «information weapons.»

Adaptation of the international law to the new challenges posed by information conflicts will involve three major aspects.

The first aspect of adaptation concerns the development of a coherent interpretation of the guiding principles of conduct of the UN member states as applied to the information domain. Such principles can could be expressed in the form of rules of conduct of nations in the field of information. One possible approach to implementing the above is represented in the draft document *International Code of Conduct for Information Security* submitted by the Russian Federation together with China, Tajikistan and Uzbekistan to the UN Secretary-General. Preparation of this document took into account the rules of conduct for member-states set-forth in the UN Charter, resolutions of the UN General Assembly concerning *Developments in Informatization and Communication in the Context of International Security* (1999–2010) and formation of a global culture of cybersecurity (2007–2009).

The second aspect of adaptation concerns formation of a system of trust between nations in the domain of information. Trust is a critical component in preventing information conflicts. The content and configuration of the system of trust requires special consideration.

The third aspect of adaptation of the international law requires a negotiated position of the UN member states towards the following:

norms of law in terms of information force and information domain and the manner of their legitimation;

the contents and the manner of legitimation of procedural norms to ascertain legal facts and coordinate international investigations;

the functions, structure and principles of operation of the international monitoring system of the global cyberspace;

the methods to make visible the objects and subjects protected by the international humanitarian law.

Regardless of the difficulties associated with preparation and conclusion of

international agreements concerning application of international law to information conflicts it is important to start this work now.

Taking into consideration the ever increasing research effort and the growing practical expertise of nations in applying information and communication technologies to exercise «force» in settling international disputes, the analysis of methods and techniques to use the leverage provided by the international law to information conflicts becomes one of the most topical tasks of the present day.

The importance of international cooperation in this area becomes more and more evident to nations of the world. It is a well-known fact that for quite a while now draft resolutions of the UN General Assembly *Developments in Informatization and Communication in the Context of International Security* proposed by the Russian Federation and a number of other countries have been passed by consensus. The UN Information Security Group of Governmental Experts (2009–2010) who prepared the report read by the UN Secretary General at the 65th session of UN General Assembly recommended in the report to "take measures to… ensure stability and reduce the risks associated with state use of information technologies.»

Legal basis for international security and peace-keeping is primarily provided by the principles and norms of international law set forth in the UN Charter, the Hague and Geneva Conventions, the rulings of the International Court of Justice, bilateral and multilateral treaties concerning security provisions.

Without doubt the above principles and norms are applicable to situations involving a breach of international peace and security through a hostile use of information technologies. At the same time, the international law appears to have certain gaps in the area in question.

Such gaps primarily concern the following issues:

qualifying information technology as a type of weapons and, consequently, recognizing attacks on information systems of critical elements of the information infrastructure of the opposing state in conflict using information technologies as an armed attack;

methods and techniques to make visible (in a tangible objective form) attacks carried out with the use of information technologies and their consequences, as well as parties who carry through such attacks;

methods and ways to ensure security of the elements of the information infrastructure used by individuals and organizations who are under the protection of the international humanitarian law including civilians, prisoners, the wounded and

the sick, the International Red Cross, as well as individuals and organizations who work to preserve cultural values;

methods and means of ensuring national neutrality in the conditions of a hostile use of information technologies by other states;

methods and techniques to prepare and bring evidence before the International Court concerning the facts of hostile use of information technologies by states with the view of breaching the sovereignty, territorial integrity and political independence of a nation.

It is worthwhile to note that the law as a mechanism for ensuring justice between parties in conflict is primarily based on the presumption of observability (the ability to register using the senses), the ability to objectively document (requires the presence of an outside observer capable of presenting evidence), and the existence of legal facts under relevant legal norms that give rise to, modify or terminate a legal relationship.

The cyberspace as the arena where "information force" is exercised including the instances of using information and communication technologies does not, however, possess the above properties.

Adaptation of the existing legal norms to the realities of the present-day shall eliminate the aforesaid gaps in the international legal regulation as regards prevention of hostile use of information technologies.

Adaptation of the international legal norms may be conducted as follows:

adaptation of the legal norms set forth in the legal sources themselves;

adaptation of the system ascertaining legal facts giving rise to, modifying, or terminating a legal relationship associated with the use of force or humanitarian protection of certain objects and subjects;

adaptation of the system of identifying the subject of hostile use of information and communication technologies;

making the objects and subjects protected by the international humanitarian law visible.

All amended legal norms and procedures as the result of the proposed adaptation must be mandatory for all the nations, otherwise such norm and procedures will be considered advisory and will fail to fill the existing gaps in the international law.

The search for proper mechanisms to adapt the international law and work out the content the adapted legal norms has already begun. Such proposals, for instance, were formulated in 2011 by the Russian Federation and a number of other nations in an official UN document *The International Code of Conduct for Information Security*. A sufficiently detailed study of possibilities for adapted legal norms governing the instances of hostile use of information technologies was conducted by an international expert group under a request from the NATO Cooperative Cyber Defense Centre of Excellence in Estonia. Their recommendations are known as *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (the Tallinn Manual).

Неманья Малисевич
(Nemanja Malisevic)
Отдел международных угроз, ОБСЕ

РАЗРАБОТКА МЕР ДОВЕРИЯ ДЛЯ СНИЖЕНИЯ РИСКОВ ВОЗНИКНОВЕНИЯ КОНФЛИКТОВ, ВЫЗЫВАЕМЫХ ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ – УРОКИ, ПОЛУЧЕННЫЕ В ОБСЕ

Очень приятно находиться здесь в окружении такого количества признанных специалистов и просто хороших знакомых. Хотелось бы поблагодарить организаторов, пригласивших меня на это мероприятие. Я здесь уже в четвертый раз, и надеюсь, как обычно, получить немало полезной информации и массу удовольствия.

Прежде чем начать, позвольте отметить, что я работаю в *Секретариате* организации, в состав которой входит 57 стран – это означает, что у меня, по сути, 57 начальников, и это помимо непосредственно директора. Как вы понимаете, всякий раз, когда в одном месте собирается столь большое количество представителей разных государств, неизбежно формируются различные позиции и предпочтения по любому обсуждаемому вопросу, и кибер/информационная безопасность в данном случае не исключение. В этой связи, поскольку меня приглашали не как независимого эксперта по кибер/информационной безопасности, а скорее в качестве представителя ОБСЕ, я не стану принимать ни чью сторону, а сохраню намеренный нейтралитет, надеюсь, вы встретите такое решение с пониманием.

В любом случае я постараюсь поделиться с вами накопленным в ходе работы в ОБСЕ практическим опытом в надежде, что он пригодится при ре-

шении столь горячо обсуждаемых на данной сессии проблем, а именно темы «Интернет – пространство свободы или новое поле боя».

Очевидно, что в ближайшем обозримом будущем справедливы будут обе трактовки. Как и в случае со многими остальными изобретениями, Интернет таков, каким его делают пользователи.

Можно провести простую параллель с химическими удобрениями. Их компоненты в равной степени подходят для выращивания сельскохозяйственных культур и для производства бомб. Пример простой, но очень доступный.

Интернет сам по себе не является злом или добром, он просто существует. Именно *пользователи* определяют, для чего он *используется*. Понятно, что, будучи вместилищем такого количества пользователей, Интернет неизбежно обретает множество предназначений и зачастую становится местом столкновения интересов. Это справедливо на самом низком уровне, т.е. на уровне индивидуальных пользователей – допустим, в ситуации, когда двое из них хотели бы зарегистрировать одинаковое доменное имя. Однако, и это вызывает мою серьезную озабоченность, действует это правило и на более высоком уровне, т.е. на этапе взаимодействия целых стран.

Проблема заключается в том, что при столкновении государственных интересов всегда есть вероятность недопонимания и эскалации.

В том, что касается кибернетических/информационных атак, государства, по очевидным причинам, являются обладателями наиболее мощных ресурсов, дающих им широчайшие возможности. Еще один интересный момент – так называемые «доверенные лица», т.е. правонарушители, которые способны действовать от имени или с фактического (или подразумеваемого) согласия государства.

Как известно, все чаще многие страны озвучивают возможность отреагировать на атаки в киберпространстве, если их результат или интенсивность становится чрезмерной, путем действий в реальном мире. Не секрет, что уже обсуждаются те предельные ситуации, в которых информационную/кибернетическую атаку можно рассматривать как основание для применения соответствующих статей международных договоренностей, связанных с физическим ответом (например, статья 5 Вашингтонского договора или статья 51 Хартии ООН). И хотя процесс далеко не завершен, он однозначно показывает значимость, придаваемую странами потенциальной эскалации угроз.

Одним из вариантов предотвращения подобного развития событий можно назвать формирование доверия между странами. Тут в игру вступают

механизмы выстраивания доверия (СВМ), важность которых сложно переоценить. В моем представлении, СВМ должны быть направлены на предотвращение ситуации, в которой атака в киберпространстве приводит к эскалации конфликта с его переносом в реальный мир посредством физического ответа. Они должны работать на минимизацию неопределенности в отношениях между странами. Я искренне полагаю эту работу ключевой, поскольку в долгосрочной перспективе неуверенная позиция стран может привести к негативным последствиям.

Держа в уме именно эти соображения, о чем многим из вас наверняка известно, страны-участницы ОБСЕ за последний год постарались согласовать первичный комплекс мер по выстраиванию доверия с целью снижения риска конфликтов на почве злоупотребления информационными технологиями и системами связи.

Это был успех сам по себе. Помнится, в прошлом году я сидел здесь же практически с пустыми руками, поскольку страны-участницы не могли договориться о формулировках при создании Неофициальной рабочей группы (IWG) для разработки указанных выше механизмов СВМ – так вышло, что это решение было принято сразу после, т.е. 26 апреля 2012 года.

В течение всего 2012 года продолжались переговоры между странами-участницами с целью принятия первого перечня механизмов СВМ на совете министров иностранных дел ОБСЕ.

Позвольте предоставить вам ряд дополнительных сведений в этой связи: рассматриваемые механизмы СВМ ориентированы на достаточно ограниченный комплекс мер обеспечения прозрачности, которые позволили бы наладить обмен информацией и связь на различных уровнях.

Применение подобных механизмов СВМ было бы добровольным, а непосредственно решение обязательным, но лишь политически, а не юридически. Скажем, каждая страна-участница могла бы определить, какой именно информацией она может поделиться, и в каком объеме хотелось бы использовать доступные каналы связи.

Первоначальный перечень механизмов СВМ предполагалось в дальнейшем обновить. Тем самым меры, не вошедшие в первый перечень, можно было бы рассмотреть позднее в ходе согласования второго, третьего и последующих перечней.

Особенность механизмов СВМ заключается в том, что соглашаясь пользоваться ими, ни одна страна не оказывается в выигрыше за счет других. В

моем представлении, все государства только выиграли бы в результате внедрения ограниченного перечня рассматриваемых механизмов.

В целом указанные механизмы СВМ стали бы первичным проявлением доброй воли в свете ухудшившихся отношений между странами на почве кибер/информационной безопасности (это касается таких проблем, как регулирование Интернета или киберпреступность).

Честно говоря, мне бы очень хотелось сегодня рассказать вам, как в ходе заседания совета министров иностранных дел ОБСЕ в Дублине в декабре месяце страны-участницы достигли консенсуса в отношении первоначального комплекса мер.

Хотелось бы отметить прекрасную работу обозначенной выше специальной группы IWG, созданной согласно решению Постоянного совета №1039 – вместе с забавными ситуациями, в которые перерастали особенно тяжелые переговоры, изобилующие подводными камнями, причем наиболее сложные случаи разрешались буквально в последнюю минуту. Затем я бы перешел к этапу реализации обозначенного первоначального комплекса механизмов СВМ, одновременно с этим изучая возможности их расширения и обновления в будущем.

Увы, этому не суждено сбыться: несмотря на достаточно схожие позиции в Дублине, консенсуса, к великому сожалению, добиться не удалось, поэтому весь гигантский труд стран-участниц и их экспертов, некоторые из которых присутствуют сегодня здесь, вложенный в прошлогодние совещания IWG, не был вознагражден.

По итогу, переговоры продолжаются.

Тем не менее, если отойти от дел прежних, хотелось бы с пользой заняться насущными вопросами и в будущем учесть все недочеты.

С моей точки зрения, необходимо выделить два ключевых момента из нашего опыта: во-первых, стоит включить все дополнительные предложения по механизмам СВМ, которые были официально направлены председателю IWG в обновленный проект перечня СВМ; во-вторых, следует запланировать намного более продолжительные встречи на высшем уровне, чтобы эксперты имели больше возможностей для всестороннего обсуждения, которое, и это мое личное мнение, абсолютно необходимо ввиду наличия в последней версии проекта ряда противоречивых позиций или таких вопросов, которые вызывают ощутимые разногласия между странами.

Перед Секретариатом была поставлена задача по оказанию поддержки

группе IWG. В этой связи, я не могу прокомментировать возможную скорость продвижения вперед по этим аспектам.

Однако, в любом случае хотелось бы поделиться с вами рядом наблюдений. Как мне кажется, обсуждение механизмов СВМ продвигается в «правильном» направлении, то есть позиции участников сближаются, по крайней мере, так было до октября прошлого года.

В дальнейшем наметилось очередное расхождение мнений, иллюстрацией чего стала последняя редакция механизмов СВМ – с дополнительными прямыми и встречными предложениями.

Подобное развитие событий отражает аналогичные обстоятельства на других международных встречах по обсуждению различных составляющих кибернетической/информационной безопасности, проводившихся в 2012 году, где позиции стран с каждым разом все ощутимее расходились.

Разница между механизмами СВМ, рассматриваемыми в ОБСЕ и обсуждаемыми на других международных форумах мерами заключается в том, что СВМ как раз призваны исключить возможное недопонимание и эскалацию отношений между странами, когда остальные подходы к решению оказываются неприменимы. Можно рассматривать их в качестве своеобразных предохранительных клапанов для сброса напряжения. По мере роста давления может потребоваться срабатывание предохранительных устройств во избежание взрыва. К тому же, и это вам подтвердит любой инженер, предохранительные устройства нужно устанавливать *до того*, как грянет кризис.

В любом случае, я остаюсь при своем мнении: в интересах всех участвующих стран разработать первый комплекс механизмов СВМ, они этого заслуживают, при этом держать в уме, что в данном случае перед нами лишь начало, а не конец переговоров. Без сомнения, в дальнейшем их надлежит обновлять и расширять. Как уже отмечалось выше, по своей сути механизмы СВМ являют собой первичное проявление доброй воли перед лицом ухудшения отношений между странами на фоне ситуации с кибер/информационной безопасностью.

Чем дальше отстоят друг от друга позиции стран, тем острее потребность в СВМ, даже несмотря на то, что достичь консенсуса становится все сложнее.

Хотелось бы надеяться, что во время встречи ведущих экспертов в этом году в Вене в рамках обсуждения работы группы IWG – желательно, как можно раньше, – они будут действовать с учетом озвученных выше соображений и с ощущением обязательности и безотлагательности, чтобы прийти к согласию в отношении первоначального комплекса СВМ.

На этом хотелось бы завершить свое выступление небольшой историей. Не так давно мне довелось встретиться за обедом с несколькими высокопоставленными дипломатами, которые хотели пообщаться на тему кибер/информационной безопасности. Один из них за десертом поделился своим опытом согласования договоренностей о разоружении, заключенных много лет назад, отметив небывалую продолжительность обсуждения. Если принять во внимание означенный опыт, с его слов, нет ни малейшего повода сомневаться в успешном завершении переговоров по кибер/информационной безопасности и связанных с этим механизмов СВМ, поскольку в сравнительном исчислении работа над ними с участием всех стран ведется достаточно непродолжительное время.

Я прекрасно понимаю, что, в понимании многосторонней дипломатии, два года – это не срок. И все же, по моим ощущениям, времени нам как раз и не хватает, по крайней мере, в сложившихся обстоятельствах этот ресурс становится бесценным. В немалой степени это связано с разрастанием непонимания между государствами по ряду ключевых проблем кибер/информационной безопасности. В результате время оказывается не на нашей стороне, когда речь заходит о внедрении механизмов, направленных на устранение разногласий и недопущение эскалации кибернетических/информационных атак, способных в потенциале вылиться в реальное, физическое воздействие. Такими механизмами и должны стать меры СВМ.

Время сейчас не на нашей стороне. Ситуация, в которой оказалась мировая общественность на данный момент, не похожа на ситуацию 2012 года. Я бы даже сказал, что она намного хуже, поскольку тон переговоров стал намного более напряженным, а позиции по отдельным аспектам обсуждаемой темы становятся все более несовместимыми.

Как мне кажется, подобное развитие событий совершенно не в интересах стран-участниц ОБСЕ!

Я искренне надеюсь, что признание преимуществ от сближения мнений в долгосрочной перспективе возьмет верх, а Секретариат ОБСЕ, в свою очередь, приложит все необходимые усилия для поддержания этого более чем целесообразного процесса.

В любом случае, от того, станут ли страны ближе друг к другу или разойдутся в стороны, во многом зависит будущее Интернета, который станет пространством свободы или полем боя.

Nemanja Malisevic
Cyber Security Officer
OSCE Secretariat
Transnational Threats Department

DEVELOPING CONFIDENCE-BUILDING MEASURES TO REDUCE THE RISKS OF CONFLICT STEMMING FROMTHE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES LESSONS LEARNED FROM THE OSCE

It is a pleasure to be here surrounded by so much expertise and familiar faces. I would like to thank the organisers for inviting me here – I think this is already my fourth visit to your event and every time I have found it both useful and enjoyable.

Before I begin, let me stress that I work for the *Secretariat* of an Organization that comprises 57 States – what this means is that, in effect, I have 57 bosses, in addition to my Director. You can imagine that whenever you have such a large group of States sitting around one table, it is almost inevitable that many different positions and preferences on any topic exist – and cyber/ICT security is no exception. As such, since I was invited not as in independent cyber/ICT security expert but, rather, as an *OSCE representative,* I will not be taking sides and will remain strictly neutral – which I am sure you will understand.

I will, nevertheless, try to share with you some lessons learned at the OSCE, in the hope that they might be beneficial for the issues this session is aiming to discuss, namely "Internet: space of freedom or new battlefield".

Clearly it is and will, likely for the foreseeable future, be both. Like so many other inventions, the Internet is what users make of it.

Much like fertiliser, for example. Do I use it for agriculture to grow crops or do I use it to make bombs – to give only one, albeit simplified, example.

The Internet is neither inherently good nor evil, it just is. Users determine what it is *used* for. Of course, with an infrastructure that is home to so many users it is inevitable that a variety of purposes will exist and, at times, this means that interests will collide and clash. This is true on the very small, individual Internet user level – e.g. when two persons want to register the same domain name. But, and this is the part that interests me, it is also true on the very big level, i.e. the interaction of States.

The problem is that whenever the interests of States clash there is always the potential for misunderstandings and escalation.

With regard to cyber/ICT attacks States are, clearly, the actors with the most resources at their command and with the highest levels of capability. An additional concern are so-called "proxies" i.e. perpetrators that could, potentially, act on behalf of or with the – actual or implied – consent of a State.

As you know, States are becoming more and more vocal about the possibility that attacks on or via cyberspace could, if they were deemed severe enough, be met with a real-world – a kinetic – response. It is no secret, for example, that the thresholds for when a cyber/ICT attack could trigger the relevant articles in international agreements related to a kinetic response are being explored (e.g. Article 5 of the Washington Treaty or Article 51 of the UN Charter). While this process is still ongoing, it clearly illustrates the importance that States attach to the potential of threat escalation.

One method to counter this development is to build confidence among States. This is where confidence-building measures (CBMs) come into play and it is one of the reasons they are so important. In my view, CBMs should work towards preventing an attack on or via cyberspace to escalate into a real-world, kinetic attack. They should work towards minimising uncertainty among States. Frankly, I believe this to be crucial work because in the long run, uncertainty among States, frequently leads to negative outcomes.

With this in mind, as most of you will know, the OSCE participating States (pS) spent last year negotiating an initial set of confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies.

This, in itself was a success. I remember sitting here, at this event, last year with somewhat empty hands because the participating States could not agree on language to create an Informal Working Group (IWG) to develop the aforementioned CBMs – incidentally, that decision was adopted just afterwards i.e. on 26th April 2012.

Throughout 2012 negotiations among participating States continued with the aim of adopting an initial list of CBMs at the 2012 OSCE Ministerial Council (MC).

Allow me to give you some additional information in this regard: The CBMs under consideration focused on a very modest set of transparency measures which would have allow for exchanges of information and communication on several levels.

Use of these CBMs would have been voluntary and the pertinent Decision politically binding rather than legally binding. Each participating State could e.g. have determined which information they would have wanted to share and to what an extent they would have wanted to use the relevant communication channels.

The initial list of CBMs was intended to be updated in the future. Therefore, measures that would not have been included in the first set could have subsequently been considered in discussions of the second, third etc. set.

It is in the nature of CBMs that by agreeing to them no State wins at the cost of another. Certainly, in my opinion, all States would have benefited from the modest set that was under consideration.

On the whole, these CBMs would have been an initial show of goodwill in light of worsening cyber/ICT security relations among States (e.g. on issues such as Internet governance, or cybercrime).

Frankly, I would have loved to sit here today and tell you how at the OSCE Ministerial Council in Dublin this past December the participating States reached consensus on this initial set.

I would have loved to showcase the good work done by the aforementioned, specifically created, IWG established by Permanent Council Decision 1039 – complete with anecdotes on a few particularly tough negotiations, sticking points and other issues that were resolved, ideally at the very last minute. I would then have outlined how we had already moved into the implementation phase of said initial set of CBMs while at the same time exploring possibilities of how to expand and update them in the future.

Alas, it was not meant to be: Even though they were close in Dublin, consensus, unfortunately, did not reward all the good work that participating States and their thematic experts – a few of which are in the room today – put into IWG meetings last year.

Negotiations, therefore, continue.

However, rather than dwell on the past I would like to build on and learn from it and look into the future.

In my view, there are two key lessons: (1) The first has been to incorporate all additional CBM proposals that were officially submitted to the IWG Chair into an updated draft set of CBMs. (2) The second has been to schedule significantly longer capital-level meetings so as to provide capital experts with the framework for in-depth discussion which – if you allow me a personal comment – will certainly be

necessary as the latest draft incorporates a number of controversial issues; or at least issues on which significant disagreement exists among States.

The Secretariat has been tasked with supporting the work of the pertinent IWG. It is, therefore, not for me to comment on the speed of proceedings.

Allow me, nonetheless, to share with you the following observation. It appears that discussions on CBMs proceeded in the "right" direction, that is, positions were moving closer together, until about October of last year.

Since then positions appear to have moved further apart and the latest version of the draft set of CBMs – with the added proposals and counterproposals – is an illustration thereof.

This development mirrors those in a number of international fora where a variety of other cyber/ICT security related issues are being discussed and where, throughout 2012, positions among States have moved further apart and continue to do so.

The difference between the CBMs pursued at the OSCE and discussions in other international fora, however, is that CBMs are exactly the type of measures that need to be in place to avoid potential misunderstanding and escalation when relations among States in other venues worsen. Think of them as pressure valves. As pressure grows you need valves to safely release it. And, importantly, as any mechanical engineer would tell you, these pressure valves need to be put in place *before* a crisis situation arises.

As such, it remains my belief that it is in the interest of all participating States to elaborate this first set of CBMs on its own merit, bearing in mind that it represents a beginning and not the end of negotiations. Clearly, they are intended to be updated and expanded in the future. As I have said before, at their core, these CBMs are an initial show of good-will in the face of worsening cyber/ICT security relations among States.

The further apart positions among States are, the bigger the need for CBMs – even though it is also more difficult to reach consensus on them.

It is, therefore, my hope that when capital experts gather in Vienna for this year's first capital-level IWG meeting – hopefully sooner rather than later – they will do so with the above in mind and with the necessary urgency as well as the will to reach agreement on an initial set of CBMs as soon as feasible.

With this in mind allow me to close with this: Not long ago, I had a lunch with several senior diplomats who wanted to exchange thoughts on cyber/ICT security. One of them, as we were eating dessert, shared his experience on negotiating

arms treaties many years ago and stressed how long these discussions had lasted. Against this experience, he said, there was no reason to be discouraged with regard to cyber/ICT security related CBMs, since States have only been working on them for a comparatively short period of time.

I appreciate that, in terms of multilateral diplomacy, two years is not a long time. Nonetheless, it is my belief that time – in general – is the one resource we do not have – and certainly not in the current circumstances. Not least because disagreements among States keep growing with regard to a number of key issues related to cyber/ICT security. As a result, time is not on our side when it comes to putting in place mechanisms aimed at preventing misunderstandings and escalation of a cyber/ICT attack, potentially even into a real-world, kinetic attack. CBMs are such a mechanism.

Time is not on our side. The situation States find themselves in today is different from 2012. I would argue that it is, actually, quite a bit worse because the tone of discussion has become more tense and positions relevant to some aspects of the thematic area have moved further apart and continue to do so.

In my opinion, this simply cannot be in the interest of any OSCE participating State!

It is my hope that recognition of the benefits of moving closer together again will prevail in the long run and the OSCE Secretariat will continue to do whatever it can to support this very worthwhile process.

In any case, whether States move closer together again or not will, ultimately, determine whether in the future we think of the Internet as primarily a space of freedom or a battlefield.

Ященко В.В.
Институт проблем информационной
безопасности МГУ имени М.В.Ломоносова

ПРОБЛЕМЫ РЕАЛИЗАЦИИ КОНЦЕПЦИИ МНОГОСТОРОННЕГО УПРАВЛЕНИЯ ИНТЕРНЕТОМ

В основу интернационализации управления сетью Интернет можно было бы положить принципы, закреплённые в итоговых документах Всемирной встречи на высшем уровне по информационному обществу (2003, 2005 гг.). К ним, в частности, относятся следующие:

• управление сетью Интернет должно быть направлено на поддержание стабильности и безопасности сети Интернет как глобального инструмента и обеспечение законности управления его использованием на основе участия всех заинтересованных сторон;

• управление сетью Интернет должно иметь многосторонний, прозрачный и демократический характер при участии правительств, частного сектора, гражданского общества и международных организаций, должно быть гарантировано справедливое распределение ресурсов, облегчать доступ для всех и обеспечивать стабильное и безопасное функционирование сети Интернет и базироваться в том числе и на Женевских принципах. Все правительства должны иметь одинаковые задачи и обязательства в сфере управления сетью Интернет на международной основе и обеспечения стабильности, безопасности и непрерывности функционирования сети Интернет;

• управление сетью Интернет должно быть открытым и гибким и содействовать созданию благоприятной среды для нововведений, конкуренции и инвестиций, повышать доверие и безопасность при использовании ИКТ путем укрепления основы для доверия.

При реализации решений в области интернационализации управления сетью Интернет важно обеспечить:

• безопасное, непрерывное и стабильное функционирование сети Интернет, защиту сети Интернет и других сетей ИКТ от возможного неблагоприятного воздействия или подверженности дополнительным рискам, для чего необходимо общее понимание вопросов безопасности сети Интернет и дальнейшее сотрудничество с целью содействия просвещению, сбору и распространению информации по вопросам безопасности, обмену передовым опытом между всеми заинтересованными сторонами в области мер по борьбе с угрозой безопасности на национальном и международном уровнях;

• стимулирование, развитие и внедрение в сотрудничестве со всеми заинтересованными сторонами глобальной культуры кибербезопасности, как это изложено в резолюции 57/239 ГА ООН и других соответствующих региональных рамочных документах, активизация международного сотрудничества и усилий на национальном уровне с целью укрепления безопасности информации личного характера, неприкосновенности частной жизни и персональных данных, а также критически важных объектов информационной инфраструктуры.

В основу механизма интернационализации управления сетью Интернет предлагается положить следующие базовые положения.

Управление сетью Интернет представляет собой разработку и применение государствами, субъектами экономической деятельности и организациями гражданского общества (при выполнении ими их соответствующей роли) общих принципов, норм, правил, процедур принятия решений и программ, регулирующих эволюцию и применение сети Интернет.

Очевидно, что не все функции управления сетью Интернет являются одинаково важными для обеспечения устойчивости функционирования глобальной информационной инфраструктуры. Если исходить из того, что основные задачи оперативного управления функционированием сети выполняются провайдерами услуг сети Интернет, то в рамках реализации мер доверия можно было бы начать обсуждение проблем:

• развития международного правового регулирования отношений в области оказания Интернет-услуг;

• определения стандартов качества этих услуг;

• интернационализации процессов принятия и реализации решений по управлению устойчивостью сети в чрезвычайных ситуациях, обусловленных влиянием факторов политического или террористического характера.

При этом важно обеспечить согласованную работу существующих негосударственных структур, реализующих сложные и наукоёмкие функции управления сетью, и вновь образуемых межгосударственных органов, компетенция которых ограничена, например, рассмотрением исключительно вопросов сохранения устойчивости функционирования сети Интернет в кризисных ситуациях.

Представляется, что основными факторами, создающими угрозы устойчивости функционирования и безопасности использования сети Интернет, являются следующие:

• уничтожение (блокирование, искажение и т.п.) операторами сети Интернет (провайдерами услуг сети Интернет) таблиц доменных имен (DNS), имеющих отношение к определенному сегменту сети Интернет;

• нарушение работоспособности программного обеспечения (внедрение вредоносных программ, искажение штатных программ управления коммуникационным оборудованием и т.п.) корневых серверов, а также программного обеспечения других серверов, используемых для осуществления коммуникационных услуг и услуг хранения данных, их содержательной обработки (так называемых «облачных вычислений») по запросам абонентов определенного сегмента сети Интернет;

• перехват, уничтожение или изменение содержания всех или части сообщений абонентов определенного сегмента сети Интернет, проходящего через коммуникационное оборудование, расположенное на территории других государств;

• включение специальных «уязвимостей» в протоколы взаимодействия коммуникационного оборудования сети Интернет, позволяющих оказывать управляемое негативное воздействие на устойчивость функционирования и безопасность использования критически важных объектов информационной инфраструктуры;

• нарушение безопасности информационных сообщений, передаваемых с использованием сети Интернет, гражданами и субъектами экономической деятельности.

Цель интернационализации управления сети Интернет должна, видимо, заключаться в уменьшении опасности угроз нарушения устойчивости функционирования и безопасности использования сети Интернет, возникающих в связи с исторически обусловленным неконтролируемым влиянием отдельных государств на принятие и реализацию критически важных для обеспе-

чения национальной безопасности как Российской Федерации, так и многих других государств, решений в области управления сетью Интернет, а также в связи с непрозрачностью процедур принятия и реализации таких решений.

Реализация функций государств в области управления сетью Интернет могла бы осуществляться на основе консенсусных решений, принимаемых уполномоченными международным договором (универсальной конвенцией) специализированными международными органами и международными организациями, в которых на равных условиях представлены все заинтересованные государства. Компетенция международных органов и организаций в области выделенных функций управления сетью Интернет закрепляется также международным договором.

Исходя из необходимости противодействия угрозам международной информационной безопасности представляется важным отнести к компетенции международных органов и организаций, образуемых государствами:

• определение правового статуса операторов сети Интернет (провайдеров услуг сети Интернет) и международно-правовой ответственности государств за обеспечение правового статуса данных субъектов;

• регулирование деятельности операторов сети Интернет (провайдеров услуг Интернет) по эксплуатации корневых серверов сети Интернет, другого коммуникационного оборудования, оказывающего влияние на устойчивость функционирования и безопасность использования сети Интернет;

• экспертизу безопасности протоколов взаимодействия коммуникационного оборудования объектов сети Интернет;

• обсуждение конфликтных ситуаций в области обеспечения безопасности функционирования и безопасности использования сети Интернет.

Для обсуждения вопросов управления сетью Интернет, относящихся к ведению субъектов экономической деятельности, и подготовки предложений по решению таких вопросов для уполномоченных органов или организаций может быть использован Форум по управлению Интернетом, созданный по результатам Всемирной встречи на высшем уровне по информационному обществу (2003, 2005 гг.).

Dr. Yashchenko V.V.,
Institute of Information Security Issues,
Lomonosov Moscow State University

ISSUES OF MULTISTAKEHOLDER INTERNET GOVERNANCE CONCEPT IMPLEMENTATION

Internationalization of the Internet governance could be based on the principles outlined in the final documents of the World Summit on the Information Society (2003, 2005). These principles are as follows:

- Internet governance should seek to support stability and security of the Internet as a global tool and ensure legitimate management of its use through participation of all parties concerned;

- Internet governance should be diversified, transparent and democratic, with participation of governments, private sector, civil society and international organizations; it should guarantee fair distribution of resources, facilitate access for all, ensure stable and secure operation of the Internet, and rely, among other things, on the Geneva principles. All governments should have identical tasks and obligations in the field of international Internet governance and enforcement of stability, security and continuity of service of the Internet;

- Internet governance process should be open and resilient and foster the development of positive environment for innovations, competition and investment, enhance confidence and security of using ICTs through consolidation of trust.

Implementation of decisions concerning the internationalization of Internet governance must imply the following arrangements:

- Secure, enduring and stable operation of the Internet, protection of the Internet and other ICT networks from potential adverse effects or exposure to additional risks, which requires a common interpretation of the matters of Internet security and further cooperation to facilitate broader awareness, collection and distribution of information on security matters, exchange of best practices among all parties concerned in respect of steps to combat security threats on the national and international levels;

- Fostering, development and introduction, in cooperation with all the parties concerned, of global cybersecurity culture, as stipulated by the UN GA Resolution 57/239 and other appropriate regional framework documents; intensification of international cooperation and national efforts seeking to enhance security

of personal information, privacy interest and private data, as well as critical information infrastructure facilities.

The procedure of Internet governance internationalization should be based on the following fundamental provisions.

Internet governance implies development and employment by the states, business entities and organizations of the civil society (performing their corresponding role) of common principles, norms, rules and procedures of arriving at decisions and implementing programs governing the evolution and use of the Internet.

Apparently, not all the functions of Internet governance are equally important for stable operation of global information infrastructure. If we proceed from the fact that basic functions of online management of the network are delivered by Internet service providers, we could start discussing the following matters as part of the confidence-building measures employment:

- Development of international regulatory management of relations in the field of Internet services;
- Setting quality standards for such services;
- Internationalization of the approval and implementation of decisions concerning the control of network stability in emergency situations caused by political or drivers or terrorism.

An important issue in this regard is to coordinate activities of non-governmental organizations entrusted with complex and high-technology functions of network management, as well as emerging international organizations whose authorities are limited, for example, to examining only the issues of maintaining stable operation of the Internet in crisis situations.

The key factors threatening the stable operation and secure use of the Internet are as follows:

- Elimination (blocking, corruption, etc.) by the Internet operators (Internet service providers) of domain name tables (DNS) that belong ot a corresponding segment of the Internet;
- Incapacitation of software (deployment of malicious codes, corruption of standard communication equipment management software, etc.) of root servers, as well as software of other servers used to provide communication services, data storage services and content-based processing of data (so-called "cloud computing") as requested by clients of a corresponding segment of the Internet;
- Interception, elimination or modification of the content of all or some messages sent by clients of a corresponding segment of the Internet transmitted

through the communication equipment located on the territory of other countries;

• Inclusion of special "vulnerabilities" in the Internet communication equipment interface protocols enabling controlled impairment of stable operation and secure use of critical information infrastructure facilities;

• Interception of data messages sent via the Internet by individuals and businesses.

Apparently, internationalization of the Internet governance must be aimed at reducing the risk of threats to stable operation and secure use of the Internet. Such threats exist due to the historical uncontrolled influence of certain countries on the adoption and implementation of decisions concerning the Internet governance that are critical to the national security of the Russian Federation and many other countries, as well as due to the non-transparency of procedures employed in the adoption and implementation of such decisions.

The states could implement their functions related to the Internet governance relying on consensus decisions made by specialized international agencies and international organizations duly authorized by an applicable international agreement (universal convention), whereby such agencies and organizations would be equally represented by all the countries concerned. The capacities of the international agencies and organizations within the scope of their assigned Internet governance functions are also stipulated by the international agreement.

Bearing in mind the importance of preventing threats to international information security, the capacities of international agencies and organizations established by the concerned countries should include:

• Determination of legal status of Internet operators (Internet service providers) and the international legal responsibility of countries for securing the legal status of such operators;

• Regulation of Internet operators' (Internet service providers') activities involving operation of Internet root servers and other communication equipment that has an impact on the stable operation and secure use of the Internet;

• Expert audits of security of the interface protocols used by the Internet communication equipment;

• Discussion of conflicts in the area of secure operation and use of the Internet.

To discuss the matters of Internet governance that are within the scope of responsibility of business entities and to prepare proposals for the authorized agencies and organizations concerning how to address such matters, the stakeholders could use the Internet Governance Forum instituted at the World Summit on the Information Society (2003, 2005).

Татьяна Тропина
Институт зарубежного и международного уголовного права им. Макса Планка, Германия

СОТРУДНИЧЕСТВО ГОСУДАРСТВА И БИЗНЕСА В БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ

1. Введение

С развитием информационных технологий вопрос борьбы с преступностью в глобальных информационных сетях выходит далеко за рамки таких проблем, как разработка норм уголовного и уголовно-процессуального права, позволяющих проводить эффективное расследование и преследование электронных посягательств. Проникновение информационных сетей буквально во все сферы жизни и возрастающая зависимость от глобальной информационной среды государства, бизнеса и общества обусловливают необходимость выработки нового подхода к обеспечению кибербезопасности. Этот подход должен учитывать, помимо трансграничной природы киберпространства, тот факт, что в информационном обмене участвует бесчисленное количество частных лиц и коммерческих компаний. Глобальные информационные сети включают все большее и большее количество взаимозависимых субъектов: сегодня безопасность пользователей и критических информационных инфраструктур зависит от компаний, владеющих сетями или являющихся поставщиками определенных услуг (банковских, финансовых, услуг связи и прочих).

Развитие информационных сетей и услуг в последние два десятилетия во многих странах было, и до сих пор остается заслугой частного бизнеса и его инвестиций. Однако в результате этого эволюция глобальных информационных технологий на несколько шагов опережает развитие принципов и моделей их регулирования. Во многих странах именно частный сектор

владеет и управляет коммуникационной инфраструктурой, являясь «двигателем» роста использования информационных технологий, в то время как на уровне государства четкое понимание того, как должны регулироваться многие аспекты киберпространства (и должны ли вообще) либо отсутствует, либо находится в зачаточном состоянии. Одним из этих аспектов регулирования киберпространства является вопрос: кто несет ответственность за кибербезопасность и как распределить ответственность по защите общественных интересов при том, что посягательства на эти интересы происходят в сетях, которыми владеет частный бизнес. Одной из последних тенденций, в связи с этим, является осознание, как на уровне государства, так и на уровне бизнеса, необходимости разработки подходов к совместной деятельности в области борьбы с преступностью и кибербезопасности.

2. Совместное регулирование и саморегулирование как модель борьбы с киберпреступностью

2.1. Модели борьбы с киберпреступностью: необходимость сотрудничества

Необходимимость привлечения бизнеса к участию в борьбе с киберпреступностью и в обеспечении безопасности в киберпространстве обусловлена децентрализованной структурой информационных сетей и их трансграничностью. Поскольку преступники могут легко обойти традиционные механизмы регулирования, например, оперируя с территории государств, где отсутствуют правовые нормы в области борьбы с электронными посягательствами, централизованное правотворчество и правоприменение, которое исторически является ядром любой концепции борьбы с преступностью в рамках государства, не может справиться с проблемой преступности в информационных сетях[93]. Интернет в целом, как децентрализованная структура, изменил традиционные модели правового регулирования с их иерархией, когда государство находится на вершине «пирамиды» управления и обладает необходимыми инструментами контроля. Эти традиционные модели не применимы к информационным сетям, поскольку в децентрализованной структуре применение старых механизмов контроля и принуждения не всегда возможно. Необходимость выработки новых способов регулирования особенно сказывается на системе борьбы с преступностью, поскольку правоприменение в сфере уголовного и уголовно-процессуального права в целом является одной из наивысших форм государственного принуждения, требующей наличия механизмов социального контроля.

[93] BROUSSEAU, E. (2002), Internet Regulation: Does Self-Regulation Require an Institutional Framework, DRUID Summer Conference on «Industrial Dynamics of the New and Old Economy - who is embracing whom?» Copenhagen/Elsinore 6-8 June 2002, P. 1

С развитием глобальных информационных сетей система противодействия преступности в киберпространстве становится все сложнее, поскольку проблема затрагивает те сферы, которые до повсеместного распространения информационных технологий относились к разным областям регулирования: например, банковская сфера и телекоммуникационные технологии. В итоге регулирующие органы могут быть наделены полномочиями, которые дублируют друг друга . В сфере борьбы с киберпреступностью и ее предупреждения это зачастую создает ситуацию, когда неясно, какой государственный орган ответственен за регулирование в определенной области и что собственно подлежит регулированию вообще[94].

Именно эта неопределенность вкупе с невозможностью применения многих традиционных иерархических механизмов контроля создает новые модели сотрудничества – как полагают некоторые исследования[95], борьба с киберпреступностью на национальном и международном уровне трансформируется в новую систему, которую правильнее называть «сетевой моделью». Эта система сфокусирована не на том, *какие субъекты (государственные органы или частные компании)* ответственны за борьбу с киберпреступностью, а на *процессах и деятельности,* необходимых для предотвращения, расследования, преследования электронных посягательств (например, создание «горячих линий» для сообщения о нелегальном контенте или действия, необходимые для борьбы с ботнетами), и *каналах обмена информацией* между участниками системы. В различных государствах участники сетевой модели могут быть разными – например, на национальном уровне борьбой со спамом могут заниматься правоохранительные органы, специальные административные органы, органы по защите прав потребителей, государственные институты по охране персональных данных и т.п. Однако в соответствии с «сетевой моделью» важен не субъект этой деятельности, а процесс сам по себе: модель отражает многообразие акторов в системе борьбы с киберпреступностью и множество подходов, но при этом акцент ставится на необходимость выполнения определенных функций (нормотворческой, контроль-

---

[94] GERCKE, M., TROPINA, T., LOZANOVA, Y. and SUND, C. (2011), The Role of ICT Regulation in Addressing Offences in Cyberspace. In: "Trends in Telecommunication Reform 2010/11. Enabling Tomorrow's Digital World". ITU, 2011.

[95] THE WORLD BANK GROUP, (n/d), Global ICT Department. Cybersecurity: A New Model for Protecting the Network, <http://siteresources.worldbank.org/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/CyberSecurity.pdf>; BRUCE, R., at al, (2005), TNO Report. International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues <http://www.ists.dartmouth.edu/library/158.pdf>

ной, превентивной, функции принуждения и т.п.) в этой области, какие бы субъекты не были ответственны за их выполнение.

Включение частного бизнеса в эту систему – необходимость, обусловленная многими факторами. Помимо общей проблемы децентрализации и трудностей применения традиционных иерархических моделей регулирования, сама природа киберпреступности с ее глобальностью, трансграничностью и быстротой передачи информации в коммуникационных сетях создает трудности для применения механизмов государственного контроля. Государство в силу ограниченности применения традиционных механизмов принуждения не может быть единственным участником, заинтересованным в борьбе с киберпреступностью, и единственным субъектом, ответственным за безопасность в глобальных информационных сетях. Высокая латентность киберпреступлений и недостаток механизмов и ресурсов со стороны государства создают ситуацию, когда правоохранительные органы могут без поддержки со стороны частного бизнеса раскрывать и расследовать только «мизерную часть»[96] от общего количества преступных посягательств, совершаемых в сети Интернет[97]. Сотрудничество с бизнесом расширяет возможности выработки новых и адаптации уже существующих механизмов противодействия преступности в киберпространстве, создавая в конечном итоге гибкий механизм контроля, позволяющий реагировать на новые способы совершения посягательств и новые угрозы[98].

Государство и бизнес в сфере борьбы с киберпреступностью дополняют друг друга в различных областях компетенции. Государство обладает необходимыми механизмами для правотворчества и правоприменения (с помощью механизмов принуждения). Частный бизнес, в силу того, что именно благодаря его участию происходит развитие и рост информационных технологий, обладает большими познаниями в этой области, и способен быстрее распознавать новые проблемы и гибче реагировать на них. Невозможно требовать от государства, чтобы оно своими силами за короткое время аккумулировало необходимые познания и нашло необходимые ресурсы для раскрытия и уголовного преследования всех посягательств в киберпространстве. Только

[96] VOGEL, J. 2007. Towards a Global Convention against Cybercrime. World Conference on Penal Law, Guadalajara, Mexico. <http://www.penal.org/IMG/Guadalajara-Vogel.pdf> , P. 5

[97] LOVET, G. 2009. Fighting Cybercrime: Technical, Juridical and ethical Challenges. Virus Bulletin Conference. September, 2009. <http://www.fortiguard.com/sites/default/files/VB2009_Fighting_Cybercrime_-_Technical,Juridical_and_Ethical_Challenges.pdf >, P. 69

[98] FAFINSKI, S., DUTTON, W. and MARGETTS, H. (2010), Mapping and Measuring Cybercrime, OII Forum Discussion Paper No 18, <http://www.law.leeds.ac.uk/assets/files/staff/FD18.pdf >, P. 19

сотрудничество с частным сектором позволит улучшить усилия государства в борьбе с киберпреступностью, именно поэтому многие страны вырабатывают модели сотрудничества с бизнесом, позволяющие обеим сторонам дополнить «сильные» стороны друг друга[99]. Утверждается, что совместное регулирование и саморегулирование в области борьбы с киберпреступностью подает больше надежд на успех, чем традиционные правоприменительные меры[100]. Различные субъекты бизнес-сообщества, оперирующие в разных сферах услуг, рассматриваются государством как критический элемент борьбы с посягательствами в киберпространстве. Помимо Интернет-провайдеров, в систему борьбы с киберпреступностью включаются компании в области электронной коммерции, мобильной коммерции, электронных платежей, разработчики приложений, поставщики оборудования[101].

2.2. Совместное регулирование: уровень интервенции со стороны государства

Совместное регулирование и саморегулирование, являясь вспомогательными источниками и формами правового регулирования, подразумевают разный уровень государственной интервенции. Поскольку совместное регулирование включает возможности прямого вмешательства государства в процесс, особенно в области применения механизмов принуждения в случае нарушений, эта форма регулирования рассматривается в качестве разновидности иерархической модели с «нисходящим» регулированием, где инициатором и гарантом исполнения является государство и его механизмы принуждения[102]. Совместное регулирование рассматривается как вспомогательные меры, которые дополняют существующие правовые нормы, установленные законом, но не являются альтернативой регулированию как механизму принуждения и контроля.

---

[99] MARSDEN C., at al. 2006. Options for an Effectiveness of Internet Self- and Co-Regulation. Phase 1 Report: Mapping Existing Co- and Self-Regulatory Institutions on the Internet. RAND Europe <http://ec.europa.eu/dgs/information_society/evaluation/data/pdf/studies/s2006_05/phase1.pdf>; SAHEL, J., (2006), A new policy-making paradigm for the Information Society, TPRC conference, 2006, <http://web.si.umich.edu/tprc/papers/2006/635/NewParadigmInfoSociety.pdf>.

[100] SIEBER, U. 2008. Mastering Complexity in the Global Cyberspace: The Harmonization of Computer-Related Criminal Law. In: DELMAS-MARTY, M. / PIETH, M. / SIEBER, U. (ed(s).): Les chemins de l'Harmonisation Pénale/Harmonising Criminal Law, Collection de L'UMR de Droit Comparé de Paris, Bd. 15. Paris, Société de législation comparée, 2008, p. 127 - 202.

[101] OECD, (2011), The Role of Internet Intermediaries in Advancing Public Policy Objectives. OECD Publishing, P. 196

[102] SENDEN, L., (2005), Soft Law, Self-Regulation and Co-Regulation in European Law: Where Do They Meet?, in "Electronic Journal of Comparative Law", vol, 9.1 (January 2005), P. 12

Саморегулирование отличается (по крайней мере, в теории) тем, что оно инициируется частным бизнесом и включает в себя меры, которые разрабатываются и устанавливаются без прямого участия государства. Государство также не имеет прямого отношения к исполнению этих мер: частный бизнес котролирует сам себя и способен в этом случае применить соответствующие механизмы принуждения в отношении субъектов, нарушающих установленные нормы поведения. Эту модель называют «восходящей», что означает, что инициатива исходит не от государства по нисходящей иерархической линии, а от бизнеса, «снизу», с точки зрения традиционных моделей регулирования[103].

В различных государствах эти две модели могут сосуществовать в разных формах, в зависимости от области сотрудничества. Совместное регулирование как более интенсивный вариант государственной интервенции существует, когда элементы сотрудничества в той или иной мере регулируются законодательством, или когда государство частично ответственно за механизмы контроля и принуждения в случае нарушения партнерами добровольно взятых на себя обязательств[104]. Степень вмешательства может быть различной: от соглашений между государством и частными компаниями, предусматривающими ответственность за их нарушение, до таких форм, как регулирование законом принципов сотрудничества между государством и частными партнерами. В некоторых случаях сотрудничество может быть обусловлено определенными пробелами в законодательстве. Например, в Нидерландах инициатива совместного регулирования процесса блокирования и удаления нелегального контента исходила от бизнес-сообщества. Однако эта добровольная мера с их стороны была обусловлена тем, что в стране были законодательно введены обязательства Интернет-провайдеров по удалению нелегального контента с мерами ответственности в случае за их неисполнение, при этом отсутствовало регулирование процедур уведомления провайдеров и удаления контента[105]. Бизнесу ничего не оставалось, как выступить с инициативой решения проблемы, не дожидаясь интервенции государства.

Интервенция государства при совместном регулировании, и даже при саморегулировании, может принимать различные формы. Государство может содействовать без прямого вмешательства созданию различных ассо-

[103] См. там же

[104] BARTLE I. and VASS P., (2007), Self-Regulation and the Regulatory State: A Survey of Policy and Practice, in „Public Administration“, Volume 85, Issue 4, December 2007.

[105] KOOP, B. J., (2010), Cybercrime Legislation in the Netherlands, in “Electronic Journal of Comparative Law”, vol. 14.3 (December 2010), <http://www.ejcl.org>

циаций, организаций и форумов. Поддержка может быть оказана при разработке соглашений между бизнесом и правоохранительными органами, при создании «горячих линий» и иных платформ для сообщения о нелегальном контенте, а также при разработке программ повышения осведомленности общества о киберпреступности.

В отличие от совместного регулирования, где государственная интервенция презюмируется в качестве необходимого компонента, саморегулирование осуществляется исключительно бизнес-сообществом, и обычно представлено в виде неиерархических организаций, таких, как ассоциации и объединения в рамках определенной индустрии. Участие этих организаций в борьбе с киберпреступностью может принимать различные формы, от сотрудничества для расследования конкретного преступления до долгосрочных программ, таких, как кодексы поведения или «горячие линии», регистрирующие сообщения о правонарушениях. Во многих странах государство так или иначе задействовано в инициативах саморегулирования, хотя зачастую без прямого участия[106] – оно может являться инициатором тех или иных программ или оказывать им поддержку, хотя сами программы осуществляются частным бизнесом.

В некоторых странах – например, в Германии, – достаточно сложно разграничить саморегулирование, совместное регулирование и государственный контроль. Так, одна из немецких программ саморегулирования была инициирована государством: в законодательстве установлено, что защита интересов несовершеннолетних в медиа-индустрии (в том числе в вопросах, касающихся вредного контента) должна осуществляться саморегулирующимися ассоциациями на основании подписанного участниками рынка соглашения. Эти ассоциации представляют собой казус, называемый «регулируемым саморегулированием» - форма самоконтроля для бизнеса была инициирована государством и установлена законом (прямая интервенция), хотя сами ассоциации действуют как саморегулируемые организации, самостоятельно разрабатывая правила поведения и следуя им[107].

---

[106] BARTLE I. and VASS P., (2007), Self-Regulation and the Regulatory State: A Survey of Policy and Practice, in „Public Administration", Volume 85, Issue 4, December 2007.

[107] BRUNST, P., and SIEBER, U. Cybercrime Legislation in Germany, in: BASEDOW/KISCHEL/SIEBER (eds.), German National Reports to the XVIII. International Congress of Comparative Law, pp. 711 – 800. Mohr-Siebeck, Tübingen 2010; MARSDEN C., at al. 2006. Options for an Effectiveness of Internet Self- and Co Regulation. Phase 1 Report: Mapping Existing Co- and Self-Regulatory Institutions on the Internet. RAND Europe, <http://ec.europa.eu/dgs/information_society/evaluation/data/pdf/studies/s2006_05/phase1.pdf>

Таким образом, обе формы участия бизнеса в регулировании чаще всего подразумевают некую вовлеченность государства, пусть даже на уровне оказания поддержки без прямого вмешательства. Поддержание инициатив бизнеса по саморегулированию и создание для него благоприятных условий – один из необходимых компонентов создания долгосрочных программ сотрудничества государства и бизнеса[108].

3. Формы сотрудничества государства и бизнеса в борьбе с киберпреступностью.

Первые инициативы сотрудничества государства и бизнеса в вопросах противодействия киберпреступности возникли в 1990-х годах и в основном включали удаление нелегального контента и «горячие» линии сообщения о детской порнографии в сети Интернет. Одной из этих программ является Internet Watch Foundation – модель «горячей линии» для сообщений о контенте, содержащем детскую порнографию, созданная в Великобритании в 1996 году при поддержке правительства. Организация финансируется провайдерами сети Интернет[109]. Развитием этой инициативы стала общеевропейская ассоциация INHOPE, созданная в 1999 году при поддержке Microsoft и Safer Internet Action Plan. Целью данной саморегулируемой организации является координация действий и повышение компетенции в сфере «горячих линий» для сообщения о нелегальном контенте[110].

Успех подобных программ дал толчок развитию идеи сотрудничества государства и бизнеса в борьбе с киберпреступностью в других областях. С развитием технологий и услуг, все большее количество коммерческих организаций, оперирующих в различных сферах «электронного» бизнеса, получает возможность внести свою лепту в борьбу с киберпреступностью[111]. Существующие ныне модели государственно-частных партнерств вышли далеко за рамки первоначальной идеи борьбы с нелегальным контентом с помощью саморегулируемых ассоциаций. Формы партнерств сегодня варьируются от участия бизнеса в расследовании конкретных уголовных дел до общенациональных государственно-частных партнерских программ кибербезопасности.

[108] OECD, (2011), The Role of Internet Intermediaries in Advancing Public Policy Objectives. OECD Publishing.

[109] AKDENIZ, Y., (2001), Internet Content Regulation. UK Government and the Control of Internet Content. In „Computer Law and Security Report“, Vol. 17, no. 5, 2001, P. 307

[110] MARSDEN C., at al. 2006. Options for an Effectiveness of Internet Self- and Co-Regulation. Phase 1 Report: Mapping Existing Co- and Self-Regulatory Institutions on the Internet. RAND Europe, <http://ec.europa.eu/dgs/information_society/evaluation/data/pdf/studies/s2006_05/phase1.pdf>

[111] OECD, (2011), The Role of Internet Intermediaries in Advancing Public Policy Objectives. OECD Publishing, P. 9

Одной из важных форм сотрудничества государства и бизнеса является принятие коммерческими компаниями кодексов, устанавливающих правила и нормы поведения в определенных обстоятельствах: например, нормы о конфиденциальности, защите данных, фильтрации контента, защите несовершеннолетних. Примерами таких кодексов являются «Кодекс поведения при уведомлении-и-удалении» в Нидерландах, направленный на регулирование поведения операторов при получении уведомления о нелегальном контенте, а также Кодекс практик в области кибербезопасности, принятый коммерческими компаниями в Австралии.

Государство и бизнес во многих странах успешно сотрудничают в создании программ повышения осведомленности населения об угрозе киберпреступности и возможности предотвращения киберпреступлений. Например, в США в 2010 году при поддержке Министерства внутренней безопасности, Федеральной торговой комиссии и коммерческих организаций была проведена кампания по он-лайн безопасности для пользователей сети Интернет[112]. Подобные кампании инициируются в настоящее время во многих странах. Они могут быть направлены на повышение осведомленности о какой-либо специфической ситуации, либо охватывать все аспекты безопасности пользователей в сети Интернет[113].

Знания и опыт частного сектора используются государством в образовательных программах повышения квалификации сотрудников правоохранительных органов и судей. Успешные инициативы в этой области включают International Centre for Missing & Exploited Children, который проводит программы повышения квалификации полиции и прокурорских работников для борьбы с детской порнографией в разных странах мира. В рамках этой инициативы Microsoft и International Centre for Missing & Exploited Children также сотрудничают с более чем 30 финансовыми институтами в разных государствах для выявления транзакций, относящихся к он-лайн преступности против несовершеннолетних[114]. Еще одна успешная инициатива – проект 2Centre, созданный в 2010 году при поддержке Европейской Комиссии и компании Microsoft, представляющий со-

[112] CISCO, (2010), Cisco 2010 Annual Security Report. Highlighting global security threats and trends. [online]. [Accessed 12 February 2012]. Available from World Wide Web: <http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2010.pdf>, P. 27

[113] CHOO, R., (2009), The organised cybercrime threat landscape, International Serious and Organised Crime Conference 2010, <http://www.aic.gov.au/events/aic%20upcoming%20events/2010/~/media/conferences/2010-isoc/presentations/choo.pdf>

[114] CHOO, R., SMITH R. and McCusker, R. (2007), Future directions in technology-enabled crime: 2007–09, Research and Public Policy Series, No. 78, Australian Institute of Criminology, Canberra, P. 94

бой сотрудничество между правоохранительными органами, частным бизнесом и образовательными организациями для проведения тренингов персонала правоохранительных органов, занимающихся расследованием преступлений.

Однако, стоит отметить, что в расследовании киберпреступлений до сих пор не существует каких-либо устойчивых партнёрских программ: в основном бизнес сотрудничает с государством при расследовании конкретных правонарушений. Это сотрудничество может быть осуществлено даже на международном уровне, как, например, совместные действия полиции США, Марокко, Турции и компании Miscosoft по выявлению создателей и распространителей вируса Zotob[115]. Однако до сих пор такое сотрудничество ведется только в рамках конкретных запросов, без каких-либо долговременных программ сотрудничества.

Тем не менее, успех многих инициатив показал, что государство и коммерческие компании могут эффективно сотрудничать в борьбе с киберпреступностью. Это привело к созданию более комплексных программ государственно-частных партнерств, особенно в области кибербезопасности и защиты критических инфраструктур. Например, в борьбе с ботнетами операторы связи стали незаменимым партнером для правохранительных органов: государственно-частные партнерства по уменьшению количества ботнетов существуют в Японии, Германии, Нидерландах, Дании и других странах[116].

Эффективность этих партнерств стала основой для создания подобных проектов и на международном уровне: например, инициатива Европейского Союза по координации усилий по борьбе с ботнетами базируется на национальных проектах государственно-частных партнерств в этой области[117].

Подобные международные проекты показывают, что следующим шагом в борьбе с киберпреступностью и повышением безопасности в глобальных информационных сетях, возможно, станут международные стратегические альянсы между государствами и коммерческими компаниями[118]. Базой для таких программ могут служить уже существующие в некоторых странах

[115] GOTLIEB, R., (2011), Cybercop Fights Organized Internet Crime, <http://www.miller-mccune.com/legal-affairs/cybercop-fights-organized-internet-crime-27897/>; LE TOQUIN, J., (n/d), Public-Private Partnerships against cybercrime, <www.oecd.org/dataoecd/51/24/42534994.pdf>

[116] ENISA, (2011), Fighting botnets: the need for global cooperation: Building on EU good practices, <http://www.enisa.europa.eu/activities/res/botnets/policy-statement>; OECD, (2011), The Role of Internet Intermediaries in Advancing Public Policy Objectives. OECD Publishing.

[117] ENISA, (2011), Fighting botnets: the need for global cooperation: Building on EU good practices, <http://www.enisa.europa.eu/activities/res/botnets/policy-statement>;

[118] CHOO, R., SMITH R. and McCusker, R. (2007), Future directions in technology-enabled crime: 2007–09, Research and Public Policy Series, No. 78, Australian Institute of Criminology, Canberra.

общенациональные программы кибербезопасности – например, государственно-частная программа «Национальная инфраструктура против киберпреступности», существующая в Нидерландах и включающая всестороннюю оценку, всесторонний мониторинг мер по борьбе с киберпреступностью и их дальнейшее развитие,[119] или австралийский проект координации действий государства и частных партнеров с помощью оперативного центра кибербезопасности, включающий в качестве частных партнеров компании телекоммуникационного сектора, банковского сектора и компании, занимающиеся поставкой воды и электричества[120]. Опыт, накопленный при реализации этих широкомасштабных программ на национальном уровне, можно использовать при создании в будущем международных государственно-частных альянсов по борьбе с киберпреступностью и поддержанию кибербезопасности.

4. Проблемы сотрудничества государства и бизнеса в борьбе с киберпрестуностью и пути их решения

Несмотря на множество успешных примеров сотрудничества государства и бизнеса в сфере противодействия киберпреступности, и государство, и частные партнеры сталкиваются с рядом проблем реализации совместных проектов.

Прежде всего, совместное регулирование и саморегулирование в сфере борьбы с киберпреступностью имеют определенные ограничения, когда дело доходит до уголовного преследования. Так, применение положений о регулировании контента, принятых бизнесом на уровне кодексов поведения, не гарантирует расследование преступлений, связанных с контентом, и наказания преступников. Некоторые виды преступлений, например, распространение детской порнографии, не могут предотвращены исключительно путем блокирования веб-сайтов или удаления информации с помощью программ сотрудничества государства и бизнеса. Государственно-частное партнерство может лишь дополнить, но не заменить необходимые уголовные и уголовно-процессуальные нормы[121].

Кроме того, саморегулирование и совместное регулирование будет эффективным при соблюдении целого ряда условий: коллективный интерес

---

[119] DEN TEKK, K. (2012), Netherlands bundles knowledge about cyber crime, <http://www.rnw.nl/english/article/netherlands-bundles-knowledge-about-cyber-crime>

[120] PARLIAMENT OF AUSTRALIA, (2010), Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime The Report of the Inquiry into Cyber Crime, Canberra, 2010

[121] GERCKE, M., TROPINA, T., LOZANOVA, Y. and SUND, C. (2011), The Role of ICT Regulation in Addressing Offences in Cyberspace. In: "Trends in Telecommunication Reform 2010/11. Enabling Tomorrow's Digital World". ITU, 2011.

в решении проблемы киберпреступности, четко определенные правила и нормы поведения, соответствие программ публично-частных партнерств ожиданиям бизнеса и общества, существование механизмов по обеспечению исполнения принятых правил (принуждение либо с помощью механизмов саморегулирования, либо с помощью интервенции государства)[122]. Отсутствие любого из этих критериев может серьезно подорвать любые программы сотрудничества. Недостаток интереса со стороны бизнеса, нехватка поддержки инициатив частных компаний со стороны государства, пассивность любой из сторон предполагаемого партнерства будет также иметь негативный эффект.

Одним из ключевых вопросов является также вопрос расходов бизнеса на программы борьбы с киберпреступностью и необходимость учитывать экономические интересы частных партнеров. Например, в Германии инициатива нескольких крупных провайдеров по установлению систем проверки возраста при доступе к контенту провалилась из-за неэффективности с точки зрения расходов для мелких операторов и отсутствия координации внутри индустрии: систему могли установить только крупные провайдеры, а недовольные нововведениями клиенты легко могли сменить провайдера услуг.[123] В Новой Зеландии, как показали экономические исследования, частный сектор рассматривает инициативы публично-частного партнерства как экономическую нагрузку, не несущую выгоды[124]. Такие же проблемы наблюдаются в США, где правительство рассматривает программы публично-частных партнерств как один из важнейших компонентов программы борьбы с киберпреступностью, в то время как коммерческие организации относятся к ним как к дополнительной экономической нагрузке, не соответствующей возможной пользе[125].

Экономически эффективные решения – один из ключевых вопросов включения индустрии в борьбу с киберпреступностью на долгосрочной основе. Государство, выдвигая инициативы по борьбе с киберпреступностью

---

122 OECD, (2011), The Role of Internet Intermediaries in Advancing Public Policy Objectives. OECD Publishing, P. 14

123 BRUNST, P., and SIEBER, U. Cybercrime Legislation in Germany, in: BASEDOW/KISCHEL/SIEBER (eds.), German National Reports to the XVIII. International Congress of Comparative Law, pp. 711 – 800. Mohr-Siebeck, Tübingen 2010

124 SHORE, M., DU, Y., and ZEADALLY, S., (2011), A Public-Private Partnership Model for National Cybersecurity, in "Policy and Internet Journal", Vol. 3, No. 2, Oxford Internet Institute/Oxford University, Berkeley Press, 2011

125 LUKASIK, S. J., (2011), Protecting Users from the Cyber Commons, in "Communications of the ACM", Vol. 54 No. 9, pp. 54-61

и поддержанию безопасности в информационных сетях, обычно подразумевает, что коммерческим организациям такие действия выгодны из соображений безопасности или репутационных соображений. Однако для частного сектора эти мотивы не являются очевидными, поскольку коммерческие организации живут по законам рынка, цены, экономической выгоды, спроса и предложения. В этой области необходим баланс, учитывающий интересы государства, коммерческих компаний и общества[126].

Ряд проблем, связанных с саморегулированием и совместным регулированием, ассоциируется с причастностью коммерческого сектора к расследованиям уголовных дел: возможности для коррупции, риск ошибок, потеря доверия, отсутствие прозрачности[127], дефицит контроля и ограниченная возможность исполнения решений в транснациональной среде, а также возможность частного сектора, а не суда, решать, какая информация должна быть удалена из сети Интернет, что может привести к частной цензуре, не имеющей лимитов[128].

5. Заключение

Саморегулирование и совместное регулирование, особенно в форме государственно-частных партнерств во многих государствах стали неотъемлемой частью стратегии борьбы с киберпреступностью[129]. Участие бизнес-сообщества, независимо от того, с чьей стороны исходит инициатива – со стороны государства или со стороны частного бизнеса – в настоящее время выходит далеко за рамки спонтанного сотрудничества с целью расследования отдельных преступлений, совершенных в киберпространстве.

Однако, несмотря на наличие подобных инициатив и программ сотрудничества, государственно-частные партнерства во многих странах сталкиваются с рядом проблем, решения которых предстоит выработать в будущем. Одна из основных проблем – отсутствие четко очерченных рамок сотрудничества, будь то правовые нормы или правила поведения партнеров при осуществле-

---

126 VAN EETEN at al, (2010), The Role of Internet Service Providers in Botnet Mitigation An Empirical Analysis Based on Spam Data, <http://www.oecd.org/LongAbstract/0,3425, en_2649_33703_46396507_119684_1_1_1,00.html>

127 CHOO, R., SMITH R. and McCusker, R. (2007), Future directions in technology-enabled crime: 2007–09, Research and Public Policy Series, No. 78, Australian Institute of Criminology, Canberra. P. 95

128 AHLERT, C., MARSDEN C.AND YUNG, C. (n/d) How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation <http://pcmlp.socleg.ox.ac.uk/sites/pcmlp.socleg.ox.ac.uk/files/liberty.pdf>, P. 27

129 UNICRI, (2010), Handbook to Assist the Establishment of Public-Private Partnerships to Protect Vulnerable Targets, UNICRI Publisher, 2010, P. 10

нии совместной деятельности. Отсутствие инициативы и интереса со стороны бизнеса, отсутствие интереса со стороны государства в поощрении частных инициатив, степень участия государства в партнерствах, которая зачастую выходит за рамки совместного регулирования и больше напоминает государственное принуждение, чем партнерскую работу, необходимость учитывать экономические интересы частных партнеров и находить взаимовыгодные решения с точки зрения расходов, вопросы доверия государства и бизнеса – лишь малая часть проблем, которые влияют на эффективность государственно-частных инициатив по борьбе с киберпреступностью.

Один из основных вопросов для государства – это поощрение интереса среди частного бизнеса к совместной работе или к самостоятельным инициативам в области расследования и преследования киберпреступлений и обеспечении безопасности в глобальных информационных сетях. Хотя в теории самостоятельное регулирование происходит исключительно по инициативе частного бизнеса, на практике эти инициативы нуждаются в государственной поддержке, которая может выражаться в создании благоприятных условий для реализации подобных проектов. Одно из необходимых условий совместного регулирования и саморегулирования – это *степень невмешательства* государства в эти инициативы, умение государства поощрять саморегулирование в области кибербезопасности, осуществлённое силами индустрии без государственного принуждения. Иначе ни о каком *само*регулировании нельзя будет говорить. Если государство использует механизмы принуждения и ответственности для привлечения частного бизнеса к сотрудничеству в борьбе с киберпреступностью, вряд ли можно назвать эти инициативы государственно-частным партнерством. *Добровольность* – ключевое слово к пониманию сути государственно-частных партнерств. Сам термин «партнерство» означает, что государство, несмотря на обладание механизмами нормотворчества, принуждения и контроля, участвует в совместном регулировании на равных, без иерархической составляющей.

Несмотря на все указанные проблемы, многие государства сегодня выходят за рамки старой системы «регулирования» и пытаются стать равным партнером частного бизнеса в борьбе с преступностью в глобальных информационных сетях, поскольку партнерство – пожалуй, единственный путь к взаимной выгоде государства, бизнеса и общества в области борьбы с киберпреступностью и обеспечения кибербезопасности.

Tatiana Tropina
Senior Researcher,
Max-Planck Institute for Foreign and International Criminal Law,
Germany

PUBLIC-PRIVATE PARTNERSHIPS IN COUNTERING CYBERCRIME

Introduction

Further development of information technologies places the problem of crime control within global information networks far beyond such measures as development of criminal code and criminal procedures that would enable efficient investigation and prosecution of electronic attacks. Penetration of information networks into practically every aspect of modern life along with the growing dependence upon the global information sphere of the state, business and society require a new approach to cybersecurity. Such approach must take into account the fact that apart from the transborder nature of cyberspace, countless number of individuals and businesses participate in the information exchange. Global information networks incorporate the ever growing number of interdependent entities: thus, security of users and critical information infrastructure depends on businesses that own the networks or are a provider of particular services (banking, financial, communication services, etc.).

The development of information networks and services over the last couple of decades has in many countries been primarily conducted and still is by the private sector and through its investments. This, however, results in the principles and models of cyberspace regulation falling several steps behind the evolution of the global information technologies. In many countries the private sector owns and operates the communication infrastructure, and provides the driver for the ever growing use of information technologies, while the state lacks a clear understanding of how to regulate many aspects of the cyberspace (and whether such regulation is altogether required). The question of who should be responsible for cyber security and how such responsibility of protecting the public interests should be distributed taking into account the fact that attacks take place in privately owned networks poses one of important problems of cyberspace regulation. One of the latest trends in this area is the recognition, both by the state and the business community, of the need to develop a common approach to oppose crime in cyberspace in collaboration.

2. Co-regulation and self-regulation as a cybercrime control model

2.1. Cybercrime control models: the need for cooperation

The decentralized composition of information networks and their cross-border nature demands help of the business community to tackle cybercrime and ensure security within the cyberspace. As criminals can easily bypass traditional regulatory mechanisms, for instance, by operating from within a nation with no legal prosecution of cyber-attacks, a centralized law-making effort and enforcement of the law, which has historically provided the cornerstone of any one nation's concept of crime control, fail to cope with the problem of crime within information networks[130]. The Internet being a decentralized system itself, defies the traditional models of legal regulation with a rigorous hierarchy where the state occupies the top of the management pyramid and has all necessary control tools. Such traditional models are not applicable to information networks, as the use of old mechanisms of control and enforcement is not always possible within a decentralized system. The need to develop new methods of regulation is especially true for the system of crime control as enforcement of penal code and procedures is one of the highest forms of public enforcement and requires mechanisms of social control.

As global information networks continue to develop, the system of crime prevention in cyberspace becomes more and more complex since the problem of security now begins to affect the areas that until the widespread of information technologies were covered by different regulatory mechanisms: for instance, the domains of banking services and telecommunication technologies. As a result of the above, regulatory authorities may be given duplicating powers. Therefore, in cybercrime control and prevention this often creates a situation where it is unclear which government agency is responsible for regulating a given area and what exactly is subject to such regulation[131].

This uncertainty coupled with the inability to apply many of the traditional hierarchical mechanisms of control gives rise to new models of collaboration (according to some studies[132]) where control of cybercrime at the national and international levels transforms into a new system which is more appropriately called the "network model". Such a system less concerned with what agents *(public authorities or private companies)* are responsible for cybercrime control, but focuses

[130] BROUSSEAU, E. (2002), Internet Regulation: Does Self-Regulation Require an Institutional Framework, DRUID Summer Conference on «Industrial Dynamics of the New and Old Economy - who is embracing whom?» Copenhagen/Elsinore 6-8 June 2002, P. 1

[131] GERCKE, M., TROPINA, T., LOZANOVA, Y. and SUND, C. (2011), The Role of ICT Regulation in Addressing Offences in Cyberspace. In: "Trends in Telecommunication Reform 2010/11. Enabling Tomorrow's Digital World". ITU, 2011.

on the *processes* and *activities* essential for prevention, investigation, prosecution of electronic attacks (for instance, launch of hot line services to report illegal content or activities in order to oppose botnets) and *information exchange channels* between the system users. Different countries might have different network model participants, for example, the national level to SPAM-control may be represented by law enforcement agencies, special administrative bodies, consumer protection authorities, public institutions for personal data protection, etc. In the network model not the agent but the process itself is of a higher importance – the model reflects the diversity of actors engaged in the cybercrime control and a variety of approaches exercised, at the same time the emphasis is given to the performance of certain functions of cybercrime control (legislature, supervision, prevention, enforcement, etc.) regardless of the actors responsible for their performance.

Engagement of the private sector by this system is a necessity conditioned by a number of factors. Apart from the general problem of decentralization and poor fitness of traditional hierarchical models of regulation, the very nature of cybercrime as a global, transborder problem with high speed information exchange within communication networks makes mechanisms of state control hard to apply. The state in view of the limited efficiency of traditional enforcement mechanisms cannot be the only actor to stand against cybercrime and cannot ensure security within global information networks on its own. High latency of cybercrime and the lack of mechanisms and resources which can be effectively exercised by the government result in a situation when law enforcement authorities without support from private businesses can but investigate and solve only a tiny fraction[133] of the total number of criminal acts committed with the Internet[134]. Collaboration with the business community would promote development of new and adaptation of existing crime control mechanisms for cyberspace which would then ultimately result in a flexible control mechanism to respond to new criminal acts and emerging threats[135].

---

[132] THE WORLD BANK GROUP, (n/d), Global ICT Department. Cybersecurity: A New Model for Protecting the Network, <http://siteresources.worldbank.org/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/CyberSecurity.pdf>; BRUCE, R., at al, (2005), TNO Report. International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues <http://www.ists.dartmouth.edu/library/158.pdf>

[133] VOGEL, J. 2007. Towards a Global Convention against Cybercrime. World Conference on Penal Law, Guadalajara, Mexico. <http://www.penal.org/IMG/Guadalajara-Vogel.pdf> , P. 5

[134] LOVET, G. 2009. Fighting Cybercrime: Technical, Juridical and ethical Challenges. Virus Bulletin Conference. September, 2009. <http://www.fortiguard.com/sites/default/files/VB2009_Fighting_Cybercrime_-_Technical,Juridical_and_Ethical_Challenges.pdf >, P. 69

[135] FAFINSKI, S., DUTTON, W. and MARGETTS, H. (2010), Mapping and Measuring Cybercrime, OII Forum Discussion Paper No 18, <http://www.law.leeds.ac.uk/assets/files/staff/FD18.pdf >, P. 19

The state and the private sector would complement each other in cybercrime control in a number of areas of expertise. The state possess necessary mechanisms for law-making and enforcement (through available mechanisms of public enforcement). The private sector in view of its key role in promoting further development and the ever growing demand for information technologies possesses greater knowledge in the area and is capable of much quicker recognition of emerging challenges and shows better flexibility in dealing with them. It is too much to ask from the state to accumulate all the required knowledge and find necessary resources over a short time and without external help to investigate and prosecute all criminal activity in cyberspace. Only joint work with the private sector shall boost the cybercrime controls exercised by the state; that is why many countries are now in search for new models of efficient cooperation with the business community which would complement each other's strengths[136]. It is argued that co-regulation and self-regulation in cybercrime control are far more promising means than traditional mechanisms of law enforcement[137]. All the various members of the business community who operate in different areas within the service market are considered by the state as a critical element in the effort to curb cybercrime. Along with Internet service providers the cybercrime control system shall incorporate businesses operating in e-commerce, mobile commerce, electronic payments, developers of applications, and hardware suppliers[138]. Ever since the first time when in early 1990's the state asked the business community and the public to help establish the so-called hotlines to report illegal content (especially as concerns child pornography) the trend for cooperation between the state and the private sector has been going up, while such cooperation itself has taken new forms and engages the ever growing number of participants in the continuous search for new approaches to talking the problem of cybercrime at the national and, more recently, international levels.

---

136 MARSDEN C., at al. 2006. Options for an Effectiveness of Internet Self- and Co-Regulation. Phase 1 Report: Mapping Existing Co- and Self-Regulatory Institutions on the Internet. RAND Europe <http://ec.europa.eu/dgs/information_society/evaluation/data/pdf/studies/s2006_05/phase1.pdf>; SAHEL, J., (2006), A new policy-making paradigm for the Information Society, TPRC conference, 2006, <http://web.si.umich.edu/tprc/papers/2006/635/NewParadigmInfoSociety.pdf>.

137 SIEBER, U. 2008. Mastering Complexity in the Global Cyberspace: The Harmonization of Computer-Related Criminal Law. In: DELMAS-MARTY, M. / PIETH, M. / SIEBER, U. (ed(s).): Les chemins de l'Harmonisation Pénale/Harmonising Criminal Law, Collection de L'UMR de Droit Comparé de Paris, Bd. 15. Paris, Société de législation comparée, 2008, p. 127 - 202.

138 OECD, (2011), The Role of Internet Intermediaries in Advancing Public Policy Objectives. OECD Publishing, P. 196

2.2. Co-regulation: government interventions

Co-regulation and self-regulation are auxiliary sources and forms of legal regulation and demonstrate different levels of government intervention. Since co-regulation implies a possibility of direct state intervention into the regulatory process, especially when exercising enforcement mechanisms in the event of a violation, such form of regulation is considered to be subtype of the hierarchy model with top-down control where the state and its enforcement mechanisms[139] have the function of the initiator and guarantor of the regulatory process. Co-regulation is rather seen as a supporting measure that complements the existing legal norms established by law and cannot replace regulation performed through the mechanism of enforcement and control.

Self-regulation differs (at least in theory) by the fact that it is initiated by a private business and includes measures that developed and implemented without any direct involvement of the state. Similarly, the state has no direct involvement in execution of such measures as the private business controls itself and is capable of applying appropriate enforcement mechanisms to actors violating applicable rules of conduct. This model is referred to as a down-top model which means that the initiative comes not from the state and down the control hierarchy, but rather comes from a business itself, from "below" as viewed by traditional models of regulation[140].

Each nation applies a particular combination of the above two models depending on the area where such cooperation is exercised. Co-regulation as an option with more intensive interventions from the state is chosen when the process of cooperation is, to a certain degree, regulated by legislation or when the state bears a partial responsibility for operation of the control and enforcement mechanisms applied in the event when partners fail to comply with their voluntary commitments[141]. The degree of intervention may vary from agreements between the state and private firms that condition liability for their violation to legislative regulation of the very principles of cooperation between the state and its private partners. In some cases such cooperation may be caused by certain legal loopholes. For instance, in the Netherlands the initiative to jointly regulate the process of blocking and removing illegal content came from the business community. At the same time, this step voluntarily taken by the private sector was due to the fact

[139] SENDEN, L., (2005), Soft Law, Self-Regulation and Co-Regulation in European Law: Where Do They Meet?, in "Electronic Journal of Comparative Law", vol, 9.1 (January 2005), P. 12

[140] См. там же

[141] BARTLE I. and VASS P., (2007), Self-Regulation and the Regulatory State: A Survey of Policy and Practice, in „Public Administration", Volume 85, Issue 4, December 2007.

that the government had passed a new law requiring Internet service providers to remove illegal content and specifying responsibility for failure to comply, whereas no regulatory procedures for notifying Internet service providers and removing such content[142] were in place. The business community had nothing to do but to take the initiative to solve the problem without an intervention from the government.

State interventions in the process of co-regulation and even self-regulation can take many forms. The state can provide assistance without a direct involvement by way of establishing associations, organizations and forums. Support may be provided in the form of assistance in working out agreements between business entities and law enforcement agencies, in launching "hot lines" and other platforms to report illegal content, as well as in developing the public cybercrime awareness programs.

In contrast to co-regulation where the state intervention is presumed as a necessary component, self-regulation is performed solely by the business community and is usually represented by non-hierarchical organizations, such as industry-specific associations and unions. The input of such organizations into the cybercrime control effort can take many forms, from cooperation aiming to investigate a specific crime to long-term programs, such as codes of conduct or "hotline" projects that record crime alerts. In many countries the state is, in one way or another, involved in self-regulatory initiatives, although its involvement is often not direct[143]: the state may initiate certain programs or render government support thereto while the programs themselves are carried out by the private sector.

In some countries, such as Germany, it is rather difficult to distinguish between self-regulation, co-regulation and government control. Thus, one of self-regulation programs in Germany was initiated by the state: the German law specifies that the minors' interests in the media industry (including matters relating to harmful content) must be protected by a self-regulating association under an agreement signed by the market players. Such associations represent a legal casus of so-called "regulated self-regulation" where the form of self-control is initiated by the state and provided by law (direct intervention), although associations themselves act as self-regulated organizations and develop their own rules of conduct and follow them on their own accord[144].

[142] KOOP, B. J., (2010), Cybercrime Legislation in the Netherlands, in "Electronic Journal of Comparative Law", vol. 14.3 (December 2010), <http://www.ejcl.org>

[143] BARTLE I. and VASS P., (2007), Self-Regulation and the Regulatory State: A Survey of Policy and Practice, in „Public Administration", Volume 85, Issue 4, December 2007.

[144] BRUNST, P., and SIEBER, U. Cybercrime Legislation in Germany, in: BASEDOW/KISCHEL/SIEBER (eds.), German National Reports to the XVIII. International Congress of Comparative Law, pp. 711 – 800. Mohr-Siebeck, Tübingen 2010; MARSDEN C., at al. 2006. Options for an Effectiveness of Internet Self- and Co-Regulation. Phase 1 Report: Mapping Existing Co- and Self-Regulatory Institutions on the Internet. RAND Europe, <http://ec.europa.eu/dgs/information_society/evaluation/data/pdf/studies/s2006_05/phase1.pdf>

Therefore, both forms of involvement of the business community in the regulatory process often imply a certain degree of participation on the part of the state, even if it is limited only to government assistance without direct intervention. Government support for business self-regulation initiatives and provision of favorable conditions for their implementation is a necessary component of long-term cooperation programs between the state and the private sector[145].

3. Forms of cooperation between the state and the business community against cybercrime

First initiatives of cooperation between the state and the business community against cybercrime were launched in the 1990's and were primarily limited to removing illegal content and establishing "hotline" services to reports child pornography on the Internet. One of such programs – the Internet Watch Foundation – is a "hotline" established in 1996 in the UK with support from the government to report content that contains child pornography. The organization is funded by Internet service providers[146]. This initiative developed later on into the pan-European association INHOPE formed in 1999 with support from Microsoft and Safer Internet Action Plan. The purpose of this self-regulatory organization is to coordinate and advance competence in operating "hotlines" reporting illegal content[147].

Successful implementation of such programs stimulated further cooperation between the state and the private sector against cybercrime on other arenas. In view of continued development of technologies and services a growing number of commercial organizations engaged in different areas of "electronic" business now have an opportunity to make their contribution into the cybercrime control effort[148]. The now existing model of public-private partnerships have gone far beyond the original idea of tackling illegal content through self-regulated association. The forms of partnerships in use today range from assistance given by the private sector in investigating specific criminal cases all the way up to national public-private cybersecurity partnership programs.

---

145 OECD, (2011), The Role of Internet Intermediaries in Advancing Public Policy Objectives. OECD Publishing.

146 AKDENIZ, Y., (2001), Internet Content Regulation. UK Government and the Control of Internet Content. In „Computer Law and Security Report", Vol. 17, no. 5, 2001, P. 307

147 MARSDEN C., at al. 2006. Options for an Effectiveness of Internet Self- and Co-Regulation. Phase 1 Report: Mapping Existing Co- and Self-Regulatory Institutions on the Internet. RAND Europe, <http://ec.europa.eu/dgs/information_society/evaluation/data/pdf/studies/s2006_05/phase1.pdf>

148 OECD, (2011), *The Role of Internet Intermediaries in Advancing Public Policy Objectives*. OECD Publishing, P. 9

One of important forms of cooperation between the state and the business community is the adoption of codes by commercial companies that set forth rules and norms of conduct for specific circumstances, such as rules of confidentiality, data protection, content filtering, protection of minors. Good examples of the above may be: the code of conduct for notification and removal of content applied in the Netherlands aims to regulate the behavior of operators in the event of notification of illegal content or the industry code of practice on cybersecurity adopted by commercial companies in Australia.

In many countries the state and the business community are successfully collaborating in cybercrime awareness and cybercrime prevention programs. For instance, in 2010 the United States launched a campaign promoting cybersecurity for Internet users[149] with assistance from the Department of Homeland Security, the Federal Trade Commission, and commercial organizations. Similar campaigns are now being actively initiated by many other nations and may be aimed at increasing public awareness of a particular problem or may cover all the aspects of user security on the Internet[150].

The knowledge and expertise accumulated by the private sector is tapped into by the state through training programs organized for officers of law enforcement agencies and judges. Successful initiatives in this area include the International Centre for Missing & Exploited Children which offers training programs for police officers and prosecutors in curbing child pornography in many countries of the world. As part of the above initiative Microsoft and the International Centre for Missing & Exploited Children collaborate with more than 30 financial institutions from different countries to identify transactions relating to online crimes against minors[151]. Project 2Centre is another successful initiative launched in 2010 with support from the European Commission and Microsoft which is a collaboration between law enforcement agencies, private businesses and educational institutions providing training to investigating officers of law enforcement agencies.

It is worthwhile to note, however, that there are still no permanent partnership programs in cybercrime investigation as the private sector tends to collaborate with the government in investigating specific crimes. Sometimes

[149] CISCO, (2010), Cisco 2010 Annual Security Report. Highlighting global security threats and trends. [online]. [Accessed 12 February 2012]. Available from World Wide Web: <http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2010.pdf>, P. 27

[150] CHOO, R., (2009), The organised cybercrime threat landscape, International Serious and Organised Crime Conference 2010, <http://www.aic.gov.au/events/aic%20upcoming%20events/2010/~/media/conferences/2010-isoc/presentations/choo.pdf>

[151] CHOO, R., SMITH R. and McCusker, R. (2007), Future directions in technology-enabled crime: 2007–09, Research and Public Policy Series, No. 78, Australian Institute of Criminology, Canberra, P. 94

such collaboration can be achieved at the international level as in the joint effort between the police forces of the USA, Morocco, Turkey and Microsoft to identify the developers and distributors of the Zotob worm[152]. So far collaboration as illustrated above continues to be exercised only under specific requests and not through long-term partnership programs.

At the same time, successful realization of many initiatives demonstrates that the government and commercial companies are capable of launching effective cooperation against cybercrime. This leads to more complex forms of public-private partnership especially in the area of cyber security and protection of critically important infrastructure. For instance, telecommunication operators have proved to be a valuable partner for the law-enforcement authorities against botnets, today a number of countries, such as Japan, Germany, the Netherlands, Denmark and others[153],have public-private partnerships formed with the object of reducing the number of botnets. High efficiency of such partnerships stimulated the launch of similar international projects, for instance, the initiative of the European Union to coordinate efforts in fighting botnets is based on national experiences of public-private partnerships in the area[154].

Such international projects demonstrate that the next step in the effort of cybercrime control and promotion of security within global information networks is likely to be in the form of international strategic alliances between national governments and commercial companies[155]. Existing national cybersecurity programs exercised by a number of countries may provide the necessary framework for such programs, for example, the public-private program National Infrastructure Against Cybercrime (the Netherlands) which provides a comprehensive assessment and monitoring of cybercrime control measures and their further refinement[156] or the Australian project in coordinating the efforts taken by the government and private partners through a

[152] GOTLIEB, R., (2011), Cybercop Fights Organized Internet Crime, <http://www.miller-mccune.com/legal-affairs/cybercop-fights-organized-internet-crime-27897/>; LE TOQUIN, J., (n/d), Public-Private Partnerships against cybercrime, <www.oecd.org/dataoecd/51/24/42534994.pdf>

[153] ENISA, (2011), Fighting botnets: the need for global cooperation: Building on EU good practices, <http://www.enisa.europa.eu/activities/res/botnets/policy-statement>; OECD, (2011), The Role of Internet Intermediaries in Advancing Public Policy Objectives. OECD Publishing.

[154] ENISA, (2011), Fighting botnets: the need for global cooperation: Building on EU good practices, <http://www.enisa.europa.eu/activities/res/botnets/policy-statement>;

[155] CHOO, R., SMITH R. and McCusker, R. (2007), Future directions in technology-enabled crime: 2007–09, Research and Public Policy Series, No. 78, Australian Institute of Criminology, Canberra.

[156] DEN TEKK, K. (2012), Netherlands bundles knowledge about cyber crime, <http://www.rnw.nl/english/article/netherlands-bundles-knowledge-about-cyber-crime>

cybersecurity operations center with private partners among telecommunication companies, banks and utilities companies providing water and electricity[157]. All the experience accumulated through such large-scale national programs can be utilized later on in international public-private alliances against cybercrime.

4. Problems associated with cooperation between the state and the private sector against cybercrime and possible solutions

Despite many successful examples of cooperation between the government and the business community in combating cybercrime, both the government and its private partners face a number of challenges in implementing joint projects.

Above all, both co-regulation and self-regulation in cybercrime control have certain limitations in terms of criminal prosecution. For instance, regardless of any existing content regulating provisions adopted by the private sector as codes of conduct, investigation and prosecution for corresponding content-related activities is never guaranteed. Some crimes, such as distribution of child pornography cannot be prevented solely by blocking websites or removing data under the programs of cooperation between the state and the business community. Public-private partnership can complement but never replace the required investigating and penal procedures[158].

Furthermore, self-regulation and co-regulation will be efficient when the following conditions are met: there is a joint interest in solving the problem of cybercrime, rules and standards of conduct are clearly defined, the established public-private partnerships comply with the expectations of the business community and the public, there mechanisms to ensure compliance with applicable rules (enforcement either through mechanisms of self-regulation, or through government interventions)[159]. Nonconformance to any of the above criteria may seriously undermine any cooperation program. The lack of interest on the part of the business community or the lack of state support of the initiatives put forth by private companies, as well as too passive a participation from any side of such partnership will have a negative effect on the program as a whole.

One of the key aspects of such partnership is the issue of cost of cyber-security programs to the business community and the need to take into account the

[157] PARLIAMENT OF AUSTRALIA, (2010), Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime The Report of the Inquiry into Cyber Crime, Canberra, 2010

[158] GERCKE, M., TROPINA, T., LOZANOVA, Y. and SUND, C. (2011), The Role of ICT Regulation in Addressing Offences in Cyberspace. In: "Trends in Telecommunication Reform 2010/11. Enabling Tomorrow's Digital World". ITU, 2011.

[159] OECD, (2011), The Role of Internet Intermediaries in Advancing Public Policy Objectives. OECD Publishing, P. 14

economic interests of private partners. For instance, the initiative of several large Internet providers in German to use age verification systems to regulate access to certain content failed owing to very high costs for small operators and poor coordination among the industry: only large providers could afford the system, while customers who did not like that innovation could easily change their Internet service provider[160]. In New Zealand, as shown by relevant economic studies, the private sector views any initiatives related to a public-private partnership as an economic burden, rather than a benefit[161]. The same problem is typical of the United States where the government considers public-private partnership programs as one of the most important components of cybercrime control, whereas commercial organizations see them as additional economic burden with benefits much less than the costs[162].

Finding cost-effective solutions is one of the keys to long-term participation of the industry in the cybercrime control effort. The government when launching initiatives to combat cybercrime and ensure security of information networks usually implies that commercial organizations should profit from improved security and better image. The above benefits might, nevertheless, be not that obvious for the private sector which operates in the market place and has to consider prices, economic benefits, the supply and demand. A good balance is required between the interests of the state, commercial companies and the public[163].

Self-regulation and co-regulation also raises a number of issues associated with the involvement of the private business in investigating crimes which offers opportunities for corruption, leads to a risk of error, loss of confidence, lack of transparency[164], lack of control and limited resources to enforce decisions

[160] BRUNST, P., and SIEBER, U. Cybercrime Legislation in Germany, in: BASEDOW/KISCHEL/SIEBER (eds.), German National Reports to the XVIII. International Congress of Comparative Law, pp. 711 – 800. Mohr-Siebeck, Tübingen 2010

[161] SHORE, M., DU, Y., and ZEADALLY, S., (2011), A Public-Private Partnership Model for National Cybersecurity, in "Policy and Internet Journal", Vol. 3, No. 2, Oxford Internet Institute/Oxford University, Berkeley Press, 2011

[162] LUKASIK, S. J., (2011), Protecting Users from the Cyber Commons, in "Communications of the ACM", Vol. 54 No. 9, pp. 54-61

[163] VAN EETEN at al, (2010), The Role of Internet Service Providers in Botnet Mitigation An Empirical Analysis Based on Spam Data, <http://www.oecd.org/LongAbstract/0,3425, en_2649_33703_46396507_119684_1_1_1,00.html>

[164] CHOO, R., SMITH R. and McCusker, R. (2007), Future directions in technology-enabled crime: 2007–09, Research and Public Policy Series, No. 78, Australian Institute of Criminology, Canberra. P. 95

internationally, as well as the rights given to the private sector to decide, without a court ruling, what information must be removed from the Internet which may result in unlimited private censorship[165].

5. Conclusion

Self-regulation and co-regulation especially in the form of public-private partnerships have become, in many countries, an integral part of the national cybercrime control strategy[166]. Participation of the business community, regardless of what side puts forth the initiative: the government or the private sector, has already gone far beyond spontaneous cooperative efforts exercised to investigate a specific crime committed within the cyberspace.

Despite of such initiatives and cooperation programs, public-private partnerships in many countries face a number of challenges solutions to which yet remain to be found. One of the biggest problems is the lack of a clearly defined scope of cooperation including appropriate legal norms and rules of conduct applied to the partners. The lack of initiative and interest on the part of the business partners, the lack of interest on the part of the government in supporting private initiatives, the degree of government involvement in such partnerships which often goes beyond co-regulation and looks like coercion exercised by the government rather than work in partnership, the need to take into account economic interests of private partners and find mutually beneficial solutions in terms of costs, the question of trust between the government and the business community – all of the above is only a fraction of the challenges that affect the efficiency of public-private cyber-security initiatives.

Despite of such initiatives and cooperation programs, public-private partnerships in many countries face a number of challenges solutions to which yet remain to be found. One of the biggest problems is the lack of a clearly defined scope of cooperation including appropriate legal norms and rules of conduct applied to the partners. The lack of initiative and interest on the part of the business partners, the lack of interest on the part of the government in supporting private initiatives, the degree of government involvement in such partnerships which often goes beyond co-regulation and looks like coercion exercised by the government rather than work in partnership, the need to take into account economic interests of private partners and find mutually beneficial

[165] AHLERT, C., MARSDEN C.AND YUNG, C. (n/d) How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation <http://pcmlp.socleg.ox.ac.uk/sites/pcmlp.socleg.ox.ac.uk/files/liberty.pdf>, P. 27

[166] UNICRI, (2010), Handbook to Assist the Establishment of Public-Private Partnerships to Protect Vulnerable Targets, UNICRI Publisher, 2010, P. 10

solutions in terms of costs, the question of trust between the government and the business community – all of the above is only a fraction of the challenges that affect the efficiency of public-private cyber-security initiatives.

One of the most important tasks the government has is to encourage private businesses to participate in joint work and put forth their own independent initiatives in investigating and prosecuting cybercrime and ensuring security of the global information networks. While in theory independent regulation is conducted at the sole initiative of the private sector, in practice such initiatives require government support which can be given by paving the way for successful implementation of such projects. One of the essential prerequisites of efficient co-regulation and self-regulation is the extent to which the government does not interfere in such initiatives that is the ability of the state to encourage self-regulation in cyber-security by the industry itself without exercising government enforcement mechanisms. Otherwise, no true self-regulation can be achieved. When the state applies mechanisms of enforcement and sets forth the responsibility of the private sector for joint work against cybercrime, such initiatives can hardly be considered a public-private partnership. Voluntary nature of partnership is the key to forming a successful public-private partnership. The very word 'partnership' means that the state, although it possesses mechanisms for law-making, enforcement and control participates in the joint regulation on equal terms without forming a command hierarchy.

Despite of all the issues mentioned above, many nations today are going beyond the old regulation system in an attempt to become an equal partner of the private sector to combat crime within the global information networks as the partnership appears to offer the only practical way to secure mutual benefit for the state, the business community and the public while prosecuting cybercrime and promoting cyber-security.

Тим Томас
(Timothy Thomas)
Старший аналитик
Управления зарубежных
военных исследований (США)

КОНЦЕПЦИЯ КИБЕР/ИНФОРМАЦИОННОГО СДЕРЖИВАНИЯ КНР

Введение

Концепция сдерживания компьютерных или информационных атак обсуждается в мировом масштабе. Обсуждаемая уже почти два десятилетия идея нередко рассматривается как далекая от реальности в связи со специфическим характером вопросов компьютерной сферы, в частности, анонимности нападающих или использования суррогатов (как людей, так и серверов). Тем не менее, американские, российские и китайские авторы пишут об этой концепции. Неизбежно ее сравнение с теорией ядерного сдерживания, которая преобладала в стратегическом мышлении почти семьдесят лет. Очевидно, что между ядерным и компьютерным сдерживанием есть существенная разница. При использовании ядерного оружия об этом факте сразу узнают все. В цифровой век в случае кибератаки могут пройти дни или недели, пока вообще станет известно, что она произошла. Может возникнуть непонимание цели кибератаки, тогда как назначения ядерного удара очевидно. Ядерные удары на данный момент наносятся государствами, а кибератака может быть результатом действий одинокого хакера, чьи намерения и местоположение могут быть тщательно замаскированы. Благодаря этим и другим немаловажным факторам идея информационного или компьютерного сдерживания по-прежнему остается концепцией противоречивой и вызывающей множество споров.

В данной статье мы уделяем основное внимание взглядам Китая на концепцию информационного или компьютерного сдерживания.[167] Изучать взгля-

[167] Термины «информационная безопасность» и «кибербезопасность», употребляемые в статье, имеют один и тот же смысл. В Китае на данный момент используются оба термина.

ды Китая и других стран важно для того, чтобы видеть, появляются ли новые ответы в задаче определения и использования положений, которые уже используют другие страны. Далее, важно понимать контекст, исходя из которого государства делают свои оценки, поскольку некоторые из них еще только развивают свои концепции компьютерного сдерживания, в то время как другие уже близки к завершению этого процесса. В заключение мы сосредоточимся на том, какие выводы можно сделать из китайской модели для данной концепции в целом. По-видимому, в Китае намереваются использовать эту концепцию для большей гибкости при проведении переговоров и получения психологического и компьютерного стратегического преимущества, возможно, и путем демонстрации силы. При этом, однако, неясно, предлагает ли китайская концепция иные способы рассмотрения самого термина.

Компьютерное сдерживание и ядерное сдерживание

С точки зрения государства есть существенная разница между концепциями сдерживания в сфере информации/компьютерной техники и ядерного вооружения. Важнейшее значение имеют хотя бы вопросы изготовления, перевозки и доставки. В случае ядерного оружия каждый шаг в процессе его применения требует множества действий. Остаться незамеченным на каждом из этих шагов неимоверно трудно. Изготовление, перевозка и доставка вызывают большую озабоченность в рамках информационной/компьютерной концепции из-за трудностей с их предсказанием. Хороший кодировщик, имеющий сведения о строении важной сети, может незаметно причинить большой вред.

Другим фактором отличия являются страдания и разрушения, связанные с атакой. Страдания, которые причиняет ядерный взрыв, хорошо известны. Мы можем изучать видеозаписи взрывов и предсказывать вероятные последствия разрушений и радиоактивного заражения. Диверсия на подводном кабеле не вызовет такой же паники, как грибовидное облако. Страдания, которые может причинить нападение в информационной/компьютерной сфере, менее предсказуемы. Непосредственными его результатами, которые можно предвидеть и ожидать, могут быть социальный хаос и психологический страх. Кибернападение на банковскую систему может на следующий день вызвать общую панику. Менее известны последствия атаки, нацеленной на цифровые устройства принятия решений, инфраструктуры промышленности или электроснабжения в зимнее время, или спутники связи. Таким образом, на ближайшее будущее не следует считать эти два типа сдерживания равными, поскольку использование оружия (ядерного) не допускается абсолютно, тогда как нападения другого типа (кибератаки) происходят каждый день в значительно меньших масштабах (обычно для целей разведки, хотя некоторые нападения уже причиняли ущерб).

Концепция ядерного сдерживания появилась уже довольно давно, и времени, чтобы обсудить ее, было достаточно. История концепции информационного/компьютерного сдерживания, связанной с технологическими разработками, значительно короче, а темп ее эволюции был и остается чрезвычайно быстрым. За последние пятнадцать лет на наших глазах появились «флешки», Facebook, YouTube и масса прочих онлайновых достижений. Выхода на сцену ждет квантовый компьютер. Прогресс в сфере кибертехнологий требует развития новых способов обеспечения сдерживания, выходя за рамки «ядерного наследия» данного понятия (или даже отказа от концепции киберсдерживания как таковой). В число новых концепций могут входить, например, способы сдерживания алгоритмических атак на компьютерные сети.

Сторонами в процессе ядерного сдерживания выступали только правительства или государства. В противостоянии при информационном или киберсдерживании стороной может быть кто угодно. Мы уже не привязаны к правительствам, послам и министерствам иностранных дел, выступающим в качестве переговорщиков по ядерному сдерживанию. Мир компьютерный резко отличается от мира ядерного в том, что экстремисты и террористы, действуя в киберпространстве, видят такие возможности, которых до сих пор им не предложила ядерная эра. При использовании ядерного оружия мы обычно знаем, кто наш противник. В вопросах информационных/компьютерных, мы знаем это далеко не всегда. Проще говоря, пришло время поговорить о том, что конкретно мы вкладываем в понятие информационного сдерживания, отвлекаясь от ядерных следов в термине «сдерживание». Информационный/компьютерный век обладает своими отличительными характеристиками, которые придется учитывать в будущем.

Еще один аспект связан с правовой стороной отличий между ядерным и информационным сдерживанием. Ограничение распространения и использования ядерного оружия уже определяется рядом договоров и положений. Создание аналогичной системы для вопросов информационного/компьютерного сдерживания остается вопросом будущего, но результаты работы множества экспертов в области права дает определенные надежды, как, например, Таллиннское руководство по международному праву, применимому к ведению кибервойны. Этот вопрос, однако, еще только должен быть раскрыт в окончательных политических заявлениях многих стран, поскольку каждое государство опасается ограничений, которые оно может взять на себя вследствие непредвиденных им обстоятельств ввиду малого практического опыта в данной области.

Киберсдерживание и Китай

С точки зрения Китая основное содержание понятия «сдерживание» заключается в использовании психологического давления или угроз, адресованных противнику. Психологический аспект сдерживания, по всей видимости, позволяет НОА Китая так смело пользоваться компьютерными методами в прямых конфронтациях, исходя из соображений риска и получаемой выгоды. Говоря о Китае, д-р Генри Киссинджер отметил склонность Мао Цзэдуна к использованию психологического аспекта сдерживания:

> С точки зрения Мао концепция сдерживания была слишком пассивной. Он был не согласен с таким положением дел, при котором Китаю приходилось дожидаться атаки. При любой возможности он стремился захватить инициативу. С одной стороны, здесь была явная аналогия с западной концепцией превентивной войны - предотвращение атаки путем нанесения первого удара. При этом, однако, согласно западной доктрине, результатом превентивных действий должны быть победа и военное преимущество. Подход Председателя Мао к превентивным действиям отличался в том, что Мао уделял чрезвычайно много внимания психологическим элементам. Его мотивом было изменение психологического баланса, не столько для поражения противника, сколько для изменения уровня предвидимых рисков[168].

Ссылаясь на разговор с бывшим китайским лидером Дэн Сяопином, Киссинджер отмечал, что тот предлагал проведение превентивной политики для противодействия любым наступательным действиям у китайской границы, которые мог бы предпринять Советский Союз. Кроме того, по словам Киссинджера, превентивная политика Дэн Сяопина была одним из аспектов китайской доктрины сдерживания с упором на наступательные средства.[169]

На данный момент неизвестно, насколько точно выполняется совет Дэн Сяопина в компьютерной области, то есть, строится ли эта работа таким образом, чтобы добиться превентивного наступательного стратегического преимущества в компьютерной сфере для противодействия компьютерному потенциалу других стран. Непрерывная обширная разведывательная деятельность Китая, однако, дает основания предполагать, что из этих наставлений сделаны соответствующие выводы. Возможно, самым важным фактором здесь является то, способна ли НОА сделать поле компьютерных

[168] Kissinger, стр. 133.

[169] Kissinger, стр. 364.

военных действий противника достаточно прозрачным или может ли она создать новые компьютерные средства вооруженной борьбы. Такое сочетание, по-видимому, имеет больше шансов добиться психологического преимущества и потенциала информационного сдерживания, чем старое понимание данной концепции. В современную эпоху действия противника уже будут сдерживаться, когда оценка риска становится проблематичной в условиях конфронтации с противником, обладающим потенциалом для наступления и дальней тактической разведки, которая предоставляет ему возможность пользоваться очевидно полной и соответствующей реальности информацией. Такой потенциал даже даст военным соединениям возможность «одержать победу, еще не вступив в бой».

За последние десять лет Китай обсуждал концепцию информационного/компьютерного сдерживания в публикуемых там книгах и журналах. В своей статье в журнале *«Китайское военное искусство»* за 2001 г., Чжао Цзиюнь, заместитель командующего Второй Артиллерийской армией (отвечающий за ядерное оружие), определяет сдерживание как «военные действия в форме демонстрации силы, которые имеют место между странами или политическими группами, или демонстрация своей решимости и готовности использовать силу с целью заставить противника отказаться от враждебных действий или наращивания применения силы.»[170]. При попытке строить предположения о том, как может выглядеть теория сдерживания кибервойны Китая статья Чжао Цзиюня является интересной отправной точкой в современных условиях.[171] В этом случае демонстрацией силы может быть простая презентация компьютерного потенциала противника.

Чжао Цзиюнь строит теорию сдерживания на сочетании определенных стратагем. Он отмечает, что ключевыми факторами в трудах Сунь Цзы, которые влияют на современную теорию сдерживания, в частности, являются превосходящая военная мощь, полная готовность к войне, наличие суровых мер наказания, превосходных навыков ведения «стратегии нападения» и «дипломатии нападения», и превращение идеологии сдерживания в ключевой элемент более сложной системы. Все эти факторы не теряют своего значения и в компьютерную эпоху. Чжао Цзиюнь добавляет, что способность противодействовать сдерживанию является

[170] Zhao Xijun, "Victory without War and Modern Deterrence Strategy," China Military Science, 2001, стр. 55-60.

[171] Ibid.

наиболее эффективным способом остановить агрессивные попытки сильных держав нанести вред национальным интересам Китая.[172]

Он заявляет, что необходимо сочетать правду с ложью - прямое применение стратагемы. Это сочетание может, вследствие запугивания сил противника с использованием психологических способов, добиться их поражения. Дружественные (китайские) силы должны искать возможности подрывать мощь и решимость сил противника, тем самым лишая его силы воли. При нанесении удара они должны делать это решительно, в первую очередь угрожая целям, имеющим наибольшую стратегическую ценность. При отсутствии дыма и пороха, именно стратегия и психология выступают в качестве средств, укрепляющих мощь и решимость в плане сдерживания.[173]

Правильная стратегия сдерживания включает в себя способность рассчитывать время и оценивать расстановку сил, с осторожностью относясь к принятию решения. Государство должно прекрасно понимать цели и задачи своей позиции в действиях по сдерживанию, чего можно добиться с помощью компьютерной разведки.[174] Чжао Цзиюнь добавляет, что Китаю следует пользоваться комплексным подходом к ситуации сдерживания. Одних лишь войск сдерживания недостаточно для обеспечения эффективности этой стратегии. Для закрепления стратегической инициативы следует задействовать все возможные силы. Эта идея заставляет вспомнить книгу Цяо Ляна и Ван Сянсуя «Неограниченная война». Эти авторы выделили двадцать четыре типа ведения военных действий, а затем выдвинули теоретическое предположение, что наибольший успех обеспечит «вкусный коктейль», т.е. сочетание этих методов.[175] Таким образом, можно представить себе, как Чжао Цзиюнь или его коллеги намереваются применять комбинацию киберспособов, которые могут послужить силой сдерживания.

В своей прекрасной работе 2001 г. “Наука о военной стратегии» издатели Пэн Гуанцянь и Яо Ючжи определяют сдерживание как «военные действия государства или политической группы, направленные на демонстрацию силы для принуждения противника подчиниться собственной воле и воздержаться от враждебных действий или эскалации проявлений враж-

[172] Ibid.

[173] Ibid.

[174] Ibid.

[175] Qiao Liang and Wang Xiangsui, Unrestricted Warfare, Pan American Publishing Company, Panama City, Panama, 2002, стр. 118.

дебности.»[176] Стратегия сдерживания предполагает наличие сил сдерживания, способных влиять на стратегическую ситуацию в целом; решимость и готовность использовать силу; и способность заставить силы противника воспринять первые два фактора и поверить в них.[177]

Военные действия, направленные на стратегическое сдерживание, определяются как «стратегический ход, предпринятый государством или политической группой с целью принуждения противника подчиниться собственной воле в рамках общей военной ситуации путем демонстрации силы или решимости в готовности применить ее.»[178] Ценнее всего в стратегическом сдерживании движущая сила, накопленная в процессе военной подготовки, демонстрации расстановки сил противнику и нанесения военных ударов.[179] Таким образом, создание этой движущей силы или ши является ценным компонентом концепции сдерживания или средств сдерживания. Ши можно также интерпретировать как энергию или стратегическое преимущество. Именно на достижение этого направлены усилия по сдерживанию, равно физические (строительство или разворачивание сил) и умственные (создание ощущения страха возмездия у противника).

Информационное сдерживание определяется в «Науке о военной стратегии» как «сдерживание, которое зависит от эффективного применения информационной науки и технологии и приводится в действие движущей силой и мощью информационной войны.»[180] В информационном мире сдерживание благодаря этой движущей силе является результатом подготовки компьютерного потенциала, демонстрации силам противника решимости или готовности кибервойск к действиям, и реальных кибератак (возможно, многочисленных разведывательных действий Китая).

Информационное сдерживание, по Пэн Гуанцяню и Яо Ючжи, характеризуется следующими чертами: во-первых, это проникновение или способность

---

[176] Peng Guangqian and Yao Youzhi, editors, The Science of Military Strategy, English Edition, The Military Science Publishing House, 2001, стр. 213.

[177] Ibid., стр. 213-214.

[178] Ibid., стр. 222.

[179] Ibid.

[180] Ibid., стр. 220. В словаре в конце английского издания «Науки военной стратегии» (перевод предоставлен китайской стороной) термин «кибер» приравнен к термину «информатизация». Это означает, что один и тот же иероглиф переводился как «кибер-» или «информатизация». По этой причине автор не видит особой разницы между киберсдерживанием и информационным сдерживанием. Соответственно, эти термины используются впоследствии взаимозаменяемо.

к проникновению не только в военные сферы, на также в политику, экономику, науку и технологию; во-вторых, трудность нахождения разницы между информационным сдерживанием и информационными наступательными действиями; в-третьих, разнообразие действий: несанкционированный вход, вредоносное ПО, разрушение БД, и т.д.; в-четвертых, двунаправленность сдерживания, при котором жертвами информационной атаки могут стать не только противники, но и третьи стороны, да и сами нападающие, вследствие взаимосвязанности локальных и глобальных сетей; и, наконец, использование средств народной войны как одного из методов ведения военных действий, т.е. возможности вступления широкой общественности в ведение боевых действий в Сети.[181]

«*Наука о военной стратегии*» отмечает также следующие аспекты, которые относятся скорее к передаче информации («передача информации является непременным условием возникновения силы и решимости, необходимых для движущей силы сдерживания)[182] при воздействия на восприятие противника:

> Тактика сдерживания требует превращения собственной силы и решимости использовать ее в информацию, передаваемую противнику и непосредственно воздействующую на его психику путем создания психологического давления, поражающего противника и внушающего ему страх... поэтому эффективное стратегическое сдерживание зависит не только от силы и решимости, но также от упомянутой выше информации, которую получает сдерживаемая сторона. Если противник не получает такую информацию или полученная им информация неточна, или сдерживаемая сторона считает, что полученная информация - не более, чем блеф и запугивание, надежного и эффективного стратегического сдерживания добиться не удастся... только если противник, получив предназначенную для его сдерживания информацию, понимает, что, если он будет принимать необдуманные решения, ему будет дан более суровый отпор, и уверен в этом, тактика сдерживания произведен необходимый эффект.[183]

Наконец, Пэн Гуанцянь и Яо Ючжи пишут, что сдерживание набирает обороты в несколько этапов: сначала усилие создается на этапе подготовки военных действий, затем усилие показывается путем демонстрации силы и дополняется нанесением военных ударов[184].

[181] Ibid., стр. 220.

[182] Ibid., стр. 215.

[183] Ibid., стр. 214.

[184] Ibid., стр. 222.

В 2003 г. в книге издателя Цай Цойхона «Информационные сети и международная политика» была предложена теория информационного сдерживания. В этой работе считается, что, в отличие от ядерного «зонта», т.е. прикрытия ядерными силами, «зонт» информационный имеет большее прагматическое значение. Информационный зонтик может теоретически дать возможность одной из сторон конфликта видеть противника, одновременно не позволяя противнику видеть действия дружественных сил. В результате контроль информации стал новой силой сдерживания. В работе Цай Цойхона говорится, что «та сторона, которая контролирует информацию, может манипулировать началом и завершением военных действий, использовать информационное оружие для того, чтобы парализовать оружие и командные системы и разрушать оружие точного наведения противника».[185]

Сетевые средства ведения боевых действий включают в себя сетевое шпионское ПО, сетевые атаки и оборонительное оружие. Ведение такого рода боевых действий подобно информационным боевым действиям.[186] Сетевые боевые действия могут проходить между государствами, государствами и организациями, государствами и отдельными лицами, между организациями, организациями и отдельными лицами и даже между отдельными лицами.[187] Сдерживающая мощь вооруженных сил Китая будет базироваться на его компьютерной мощи, производительности и надежности каналов связи, потенциале ведения разведывательных действий в режиме реального времени, способности проводить компьютерное моделирование и других информационных компонентах. Эти элементы могут играть сдерживающую роль, пользуясь ложными представлениями противника и оказывая на него психологическое давление[188] благодаря управлению информацией. Цай Цойхон добавляет здесь еще более настораживающее мнение: по его оценке, «информационная сетевая война в условиях ядерного сдерживания станет новой формой международных конфликтов в будущем.»[189]

В 2004-м году журнал «*Китайская военная наука*» опубликовал несколько статей на тему стратегического сдерживания, из которых можно понять, как это будет выглядеть применительно к компьютерной сфере. Чжоу Пэн и

---

[185] Cai Cuihong, Information Networks and International Politics, [изд. неизвестен], 2003, стр. 163.

[186] Ibid., стр. 173.

[187] Ibid., стр. 176.

[188] Ibid., стр. 178.

[189] Ibid., стр. 172.

Вэн Энбин из Военной научной академии считают, что под стратегическим сдерживанием понимаются «военные действия государства или политического блока, нацеленные на то, чтобы принудить противника не отважиться на враждебные действия или обострение конфликта путем демонстрации силы или указания на решимость и готовность использовать силу, в результате чего достигаются конкретные стратегические цели.»[190] Наличие военной мощи является обязательным условием, наравне с готовностью использовать силу и способностью добиться того, чтобы объекту сдерживания стал известен потенциал противника. Целенаправленное сдерживание может быть результатом управляемости и гибкости информационных действий.[191] Таким образом, в компьютерный век сила может быть продемонстрирована другому государству просто путем демонстрации контроля над какой-либо сетью.

По мнению Чжоу Пэна и Вэн Энбина, предыдущий президент Китая Цзян Цзэминь рекомендовал поднять сдерживание до уровня стратегии. Концепция стратегического сдерживания может использоваться для ограничения возможности войны, отсрочки начала военных действий или предотвращения их эскалации. Ядром нового сдерживающего потенциала должна быть технология «булавы убийцы». Цзян Цзэминь подчеркнул, что приоритетным направлением новых разработок должны быть мобилизационные мероприятия. С этого момента Китай не переставал организовывать широкие процессы информационной мобилизации, проводя соответствующие военные и гражданские учения неоднократно и ежегодно. Китай «должен создать боевые соединения чрезвычайной мобилизации» в связи с высоким темпом ведения технологических войн и, соответственно, требованиями моментально быть готовыми к ведению таких действий. В информационный век начало войны может иметь решающее значение. Мобилизационный потенциал дает Китаю возможность прибегать к сдерживающему эффекту народной войны в условиях высоких технологий.[192] Такими боевыми соединениями чрезвычайной мобилизации может быть компьютерное ополчение, уже созданное в Китае, или масса других компьютерных подразделений.

С точки зрения Чжоу Пэна и Вэн Энбина, военные силы общенационального масштаба создают эффект надежного сдерживания, который должен быть наращен сейчас, за период так называемого двадцатилетнего «окна

---

190 Zhou Peng and Wen Enbin, "Developing a Strategic Deterrence Theory with Chinese Characteristics," China Military Science, No. 4 2004, стр. 19.

191 Ibid., стр. 20.

192 Ibid., стр. 22.

стратегических возможностей» Китая. Эффективные силы сдерживания включают в себя использование ядерного сдерживания, сдерживания традиционных видов ведения боевых действий, сдерживания войны в космосе и информационное сдерживание, что снова заставляет нас вспомнить о концепции «коктейля» методов ведения войны.[193] Авторы добавляют, что «Кульминацией стратегического руководства становятся правильные выбор и постоянное обновление форм сдерживания; это наиболее реальная и самая динамичная составляющая стратегии сдерживания.»[194]

Вторая статья в «*Китайской военной науке*» от 2004 г. за авторством группы исследователей из Военной научной академии (ВНА) также посвящена стратегическому сдерживанию. Авторы отмечают, что для успешного сдерживания нация должна располагать адекватными силами, решимостью их использовать и способностью заставить противника поверить, что эти предпосылки существуют.[195] То, что многие страны обвиняют Китай в ведении масштабных разведывательных операций в коммерческих фирмах во всем мире, указывает на то, что они могут быть задействованы в процессе создания именно такой формы сдерживания.

Группа исследователей из ВНА указала, что для достижения всестороннего сдерживания нужно сочетание средств ядерной, традиционной, космической, народной и информационной войны. Последний элемент особенно важен. Он пронизывает любые прочие формы сдерживания и означает как психологическую двойственность, так и несходство использования физического или функционального поражения. Для стратегического сдерживания важнее всего, по мнению авторов, усилие, порожденное военной подготовкой, демонстрация наличия сил противнику, и способность вложить это усилие в военные удары.[196] Китай продемонстрировал подготовку информационного ополчения и предполагаемую способность вторгаться в чужие системы и продолжает обновлять свои военные силы.

В 2007 г. генерал-майор Ли Дейи утверждал, что информационное сдерживание выйдет на уровень, сравнимый с уровнем ядерного сдерживания. Новые и важные способы сдерживания будут включать в себя технологическое, оружейное и ресурсное сдерживание в информационной сфере. Да-

[193] Ibid., стр. 24.

[194] Ibid., стр. 25.

[195] Academy of Military Science Research Group, “Strategic Deterrence,” China Military Science, No. 5 2004, стр. 143.

[196] Ibid.

лее, создание и использование контрсредств сдерживания будут элементом нового образа мышления Китая.[197] Также в 2007 г. старший полковник Дэн Йифэй писал, что информационное сдерживание станет средством, вслед за ядерным сдерживанием, достижения национальных и военных стратегических целей. Он считает, что именно информация становится важным концептом военной мысли. С его точки зрения, сражение за информационное превосходство и формирование потенциала информационного сдерживания – ключевые моменты военной мысли на данный момент.[198]

В 2009 г. несколько представителей высшего генералитета ядерных войск Китая писали о том, как соотносятся информационные ресурсы и информационные компоненты вооружения с информационным сдерживанием. Чжоу Фаньинь отмечал, что в информационном веке концепция информационного сдерживания определяется как принуждение противника сложить оружие путем демонстрации или подчеркивания особой точности средств вооружения дружественных сторон.[199] Пример Чжоу Фаньиня заставляет читателя поверить в то, что он, разумеется, говорит скорее о точности наведения оружия, чем о кибератаках на инфраструктуру.

«Air & Space Power (Воздушные и космические силы)» *писала, что Китай продолжит использовать стратегию сдерживания на самом высоком уровне, полагаясь на «неопределенность» для большего сдерживающего эффекта.*[200] Даже хотя ее комментарий относился к ядерному сдерживанию, он может легко применяться и к сценарию сдерживания информационного. В век компьютерного хакерства «неопределенность» фактической личности хакера или связи с правительством является, возможно, самым большим препятствием, которое придется преодолевать тем, кто будет атакован или подвергнется разведывательным действиям в рамках данной концепции.

Кроме того, в 2010 г. китайские аналитики Тэн Лян и Чжанг Цзин выступили на конференции, проводившейся Институтом Восток-Запад, с докладом «Может ли сработать киберсдерживание?». Они считают, что анонимность,

---

[197] Li Deyi, "A Study of the Basic Characteristics of the Modes of Thinking in Informatized Warfare," China Military Science, No. 4 2007, стр. 101-105.

[198] Deng Yifei, "A Revolution in Military Thinking in the Information Age," China Military Science, No. 6 2007, стр. 71-78.

[199] Zhou Fangyin, "The Effect of the Information Revolution on Military Affairs and Security," Beijing Xiandai Guoji Guanxi, 1 August 2001, стр. 28-32.

[200] Yao Yunzhu, "China's Perspective on Nuclear Deterrence," Air & Space Power Journal, Spring 2011, стр. 30.

глобальный охват, рассеянность и взаимосвязанность сетей и Интернета снижает эффективность киберсдерживания и даже могут «сделать его абсолютно бесполезным.»[201]. Эти факторы еще дальше уводят компьютерное сдерживание (киберсдерживание) от факторов, связанных со сдерживанием ядерным, не говоря уже о том, что кибератаки, по сравнению с ядерными ударами, обходятся куда дешевле и связаны с куда меньшими рисками. Тэн Лян и Чжанг Цзин отметили, что «основной проблемой киберсдерживания являются косвенные повреждения».[202] Они также добавили следующие соображения: понятие взаимного гарантированного уничтожения не применимо к киберсдерживанию; важнейшими препятствиями на пути организации киберсдерживания являются технические сложности, отсутствие социальной ответственности и понимания важности безопасности, неадекватное международное сотрудничество (особенно нежелание государств «поступиться собственными предполагаемыми интересами в киберпространстве или различиями, которые могут существовать в их законодательстве или нормах права»), а также отсутствие ясной позиции в отношении того, что является противозаконной и вредоносной информацией, в связи с различным пониманием свободы распространения информации или других обычаев и традиций.[203] Таким образом, эти авторы подчеркивают неспособность данной концепции справиться с современными техническими сложностями.

В 2011 г. в китайских СМИ появились несколько статей об информационном/компьютерном сдерживании. В одной статье в авторитетном издании «*Китайская военная наука*» отмечалось, что главный военный потенциал Китая базируется на способности выигрывать локальные войны в условиях информатизации. Этот потенциал поддерживается силой сдерживания. Авторы статьи, Лю Йонминь и Цзин Чжэнцинь отмечают следующие факторы, говоря об оборонном и наступательном потенциале Китая:

> способность обеспечивать эффективное стратегическое информационное сдерживание; способность находить информационные узлы операционных систем противника, проникать в них, и повреждать и контролировать их; способность физически разрушать информационные системы противника; способность организовывать сетевые атаки на компьютерные сети противника; способ-

[201] Tang Lan and Zhang Xin (edited by Andrew Nagorski), “Can Cyber Deterrence Work?” East West Institute Conference, April 2010, стр. 1.

[202] Ibid.

[203] Ibid., стр. 2.

> ность защищаться от разведывательных информационных действий противника; способность сопротивляться информационным вторжениям противника; и способность перестраивать информационные системы. [204]

Во многих статьях в 2011 г. обсуждалась киберстратегия США, опубликованная в это время. Комментарии в отношении использования Соединенными Штатами концепции киберсдерживания были крайне отрицательными. В одной из этих статей отмечалось следующее по поводу того, что США будут предположительно полагаться на киберсдерживание в будущих войнах:

> Идея так называемого «киберсдерживания», которую предлагают высшие военные чины США, более или менее та же, что и «ядерное сдерживание», предлагавшееся в прошлом... Что касается Соединенных Штатов, «киберсдерживание» может состоять из трех компонентов: Во-первых, киберармия, способная как на оборонительные, так и на наступательные действия; во-вторых, развитие вооружения, включая «цифровые бомбы», используемые в кибератаках; и в-третьих, если необходимо, использование реальных военных сил для нанесения ударов по сетям противника. Для Соединенных Штатов или небольшой группы государств будет невозможно монополизировать эти три компонента, поскольку первые два могут быть получены даже в индивидуальном порядке или могут быть легко сымитированы.[205]

В другой направленной против США статье 2011 г. отмечается, что «эффективность киберсдерживания вызывает вопросы из-за специфики, сложности и проблематичности кибертехнологий. Более того, теория сдерживания обострила атмосферу международного недоверия и неуверенности и, таким образом, повредила международному сотрудничеству в киберпространстве».[206]

В 2012 г. и начале 2013 г. авторы китайских статей, по всей видимости, начали отходить от концепции информационного/компьютерного сдерживания. Вместо этого, сдерживание начали соотносить с «победой в локальных войнах в условиях информатизации». Например, в статье, в которой описы-

---

[204] Liu Yongming and Jin Zhenxing, "Study on Hu Jintao's Important Instructions on Enhancing Capabilities of Accomplishing Diversified Military Tasks with Winning Local Wars under Informatized Conditions as the Core," China Military Science, No. 6 2011, стр. 1-9.

[205] Yu Xiaoqiu, "Cyber Deterrence Is a Dangerous Game," Renmin Ribao Online, 25 July 2011, стр. 3.

[206] Без авторства, "Reality of the Virtual World," China Daily Online (in English), 16 July 2011.

валось открытие в 2013 г. первой сессии 12 Всекитайского собрания народных представителей, упоминалось, что «в 2012 г. продолжал укрепляться потенциал сдерживания и боеспособность в условиях информатизации».[207] Старший полковник Сюй Вэйди в своей статье о военном сдерживании, опубликованной в 2012 г. в американском журнале «Air and Space Power», отмечал следующее:

> Другими словами, на протяжении всего периода «холодной войны», в то время как западные державы говорили о сдерживании, они нередко прибегали к принуждению. Это искаженное и извращенное «сдерживание» лучше всего демонстрирует то, что они сделали с обороной на передовых рубежах, заняв оборонительную позицию, в которой говорят об обороне, лишь «приставив штык к горлу врага».[208]

Тем не менее, концепция принуждения упоминалась и применительно к китайской военной мысли. В статье Дина Ченга, американского эксперта по военным делам Китая, отмечалось, что в Энциклопедии НОА стратегия сдерживания или «вейше жаньлуэ» определяется как «демонстрация военной мощности, или угроза применения военной мощи для принуждения противника к капитуляции».[209] Таким образом, становится очевидно, что идея принуждения не чужда концепции сдерживания НОА. Некоторые аналитики в США даже переводят название китайской концепции сдерживания как «принуждение».

Заключение: Помог ли Китай в ходе обсуждения?

Основные выводы, которые можно сделать из вышесказанного:

• Сдерживание можно определить как военные действия, принимающие форму демонстрации силы.

• При отсутствии дыма и пороха, стратегия и психология выступают в качестве средств, укрепляющих мощь и решимость в плане сдерживания.

• Новые и важные способы сдерживания будут включать в себя технологическое, оружейное и ресурсное сдерживание в информационной сфере. Информационное сдерживание поднимется до стратегического уровня, при-

---

[207] Без авторства, “Rally Wisdom and Forces to Hold Up the ‘China Dream,’” Jiefangjun Bao Online, 5 March 2013, стр. 1.

[208] Xu Weidi, “Embracing the Moon in the Sky or Fishing the Moon in the Water?” Air & Space Power Journal, July-August 2012, стр. 16.

[209] Dean Cheng, “Chinese Views on Deterrence,” Joint Force Quarterly, Issue 60, First Quarter, 2011, стр. 92.

ближающегося к уровню ядерного сдерживания, став способом достижения национальных и военных стратегических целей.

• Эффективные силы сдерживания включают в себя использование ядерного сдерживания, сдерживания традиционных видов ведения боевых действий, сдерживания войны в космосе и информационное сдерживание, что снова заставляет нас вспомнить о концепции «коктейля» методов ведения войны.

• Сторона, которая контролирует информацию, может манипулировать началом и завершением военных действий, использовать информационное оружие для того, чтобы парализовать оружие и командные системы и разрушать оружие точного наведения противника.

• Сдерживающая мощь вооруженных сил Китая будет базироваться на его компьютерной мощи, производительности и надежности каналов связи, потенциала ведения разведывательных действий в режиме реального времени, способности проводить компьютерное моделирование и других информационных компонентах. Эти элементы могут играть сдерживающую роль, пользуясь ложными представлениями противника и оказывая на него психологическое давление.

• Под стратегическим сдерживанием понимаются «военные действия государства или политического блока, нацеленные на то, чтобы принудить противника не отважиться на враждебные действия или обострение конфликта путем демонстрации силы или указания на решимость и готовность использовать силу, в результате чего достигаются конкретные стратегические цели».

• Сдерживание противника будет успешным, если его попытка оценить риски становится проблематичной в результате того, что он сталкивается с противником, располагающим информацией наступательного характера, по всей видимости, достаточно полной и выглядящей реалистичной.

• На данный момент непонятно, насколько буквально деятельность Китая в компьютерной сфере будет соответствовать завету вождя Дэна Сяопина, данному в 1990-х, а именно, настроен ли он на создание превентивного стратегического преимущества в компьютерной сфере.

Некоторые пункты из этого списка имеют значение для понимания китайской концепции киберсдерживания. Первым является сосредоточенность Китая на использовании стратегии и психологии в применении своей теории сдерживания. Эта сосредоточенность отражает давний интерес Китая к этим темам. Другим государствам следует делать свои оценки в дан-

ном контексте, когда они пытаются понять китайский подход к киберсдерживанию, чтобы понимать, что значат эти термины и как они влияют на оценки риска Китаем. Во-вторых, по всей видимости, Китай рассматривает современную ситуацию со сдерживанием в зависимости от интеграции в нее различных типов и видов сдерживания, в частности, в сферах космического, традиционного и информационного вооружения, что в конечном итоге приводит к успешности стратегического сдерживания. Эта интеграция концепций продвигалась, начиная с 1999 г., хотя и другие способы ведения войны не оставались без внимания. В-третьих, Китай считает, что надежность сдерживания повышается благодаря количественной оценке компьютерного потенциала, надежности информации и других факторов. Эти факторы можно рассматривать и рассчитывать по неким закрытым формулам, применяемым в Китае, в частности, для оценки общего потенциала государства. В-четвертых, как и с другими формами сдерживания, Китай понимает, что киберсдерживание может оказаться эффективным только при демонстрации адекватного цифрового потенциала, которым он может воспользоваться для запугивания или сдерживания других по мере необходимости. Такая демонстрация силы может быть даже раскрытием в цифровой форме добытых пиратским способом секретов, что, например, случилось во время фиаско с Wikileaks. Наконец, китайские авторы считают, что государство должно быть способным продемонстрировать, что оно управляет информацией, если собирается поддерживать стабильность в цифровых аспектах своей жизнедеятельности и успешно манипулировать началом и окончанием сценария типа сдерживания. Хотя все эти пункты принимаются достаточно хорошо, статьи 2011 г. указывают на то, что в Китае существует негативное отношение к киберсдерживанию в связи с киберстратегией США. Концепция сдерживания, при этом, привлекательна для китайцев, если она привязана к победам в местных войнах в условиях информатизации.

В целом, китайские теоретики предложили несколько направлений, в которых другие государства могут думать над развитием концепции киберсдерживания. Сущность практики сдерживания Китая, по-видимому, сводится к разрешению военных ситуаций невоенными способами и применения таких стратагем, как победа без битвы и победа до вступления в бой. Киберсдерживание китайского толка имеет стратегический характер, а обсуждение этой темы китайскими специалистами указывает на то, что рассматриваются различные типы киберсдерживания или информационного сдерживания. Далее, китайские теоретики понимают, что из-за быстрого темпа высокотехнологичных войн решающее значение может иметь начало

войны. По этой причине Китай «должен создать боевые соединения чрезвычайной мобилизации», если ему придется бросить силы народного ополчения на борьбу с противником в условиях технологического противостояния. Китайцы добавляют, что они должны приготовить силы контрсдерживания для ответа на любые действия потенциального противника. Под этим может пониматься, в частности, использование военных учений для демонстрации силы в использовании технологических решений или, возможно, даже раскрытия разведывательной деятельности, чтобы доказать, что противник бессилен остановить эти действия, или довести это до его сведения.

В общем, Китай уже обсуждал стратегическую политику информационного/компьютерного сдерживания, которая заставила бы другие страны гадать, на что направлена политика сдерживания. Эта политика, как и в случае ядерного сдерживания, основана на идее неизвестности, которая позволяет добиться большей эффективности сдерживания. Ситуация Китая отличается от ситуации и США, и России, и это следует принимать во внимание, когда другие страны оценивают окончательные цели и соображения китайской стороны при обдумывании использования этой концепции. Она представляет собой способ, которым НОА может сохранить боеспособность и возможность контролировать военные, суверенные и экономические вопросы. Тем не менее, китайский подход оказался полезным, предоставив другим странам отличный взгляд или способ обдумывать сдерживание. Самым важным здесь остается избежать конфликта. НОА, очевидно, рассчитывает, что политика прочного киберсдерживания поможет Китаю найти время и средства, чтобы реализовать военный аспект «китайской мечты» нового президента Си Цзиньпина.

ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ: Взгляды, изложенные в данном отчете, принадлежат автору и не обязательно представляют собой официальное мнение или позицию Министерства сухопутных войск, Министерства обороны или Правительства США.

Управление зарубежных военных исследований (FMSO) проводит оценку региональных вопросов военных проблем и вопросов безопасности путем изучения открытых источников и прямого взаимодействия с зарубежными военными специалистами и экспертами по безопасности других стран, выступая советниками командования вооруженных сил по вопросам политики и планирования, имеющих особую значимость для вооруженных сил США и остального военного сообщества.

Timothy Thomas
Senior analyst, Foreign Military Studies Office, USA

CYBER/INFORMATION DETERRENCE: HOW DOES CHINA VISUALIZE THE CONCEPT?

Introduction

The concept of cyber or information deterrence is being debated worldwide. While discussed for almost two decades, the idea is often viewed as unrealistic due to the specific characteristics of cyber issues, such as the anonymity of attackers or the use of surrogates (both individuals and servers). Regardless, American, Russian, and Chinese authors all write on the concept. Inevitably, comparisons are made to the theory of nuclear deterrence, which has dominated strategic thought for nearly seventy years. There are, obviously, striking differences between nuclear and cyber deterrence. If a nuclear weapon was involved, everyone would know about the incident. In the digital age, when a cyber attack occurs, it may take days or weeks to even know it has occurred. Misunderstandings can develop as to the intent of a cyber attack, while the intent of a nuclear attack is transparent. Nuclear attacks are conducted by nation-states at the present time, while a cyber attack can be initiated by a lone hacker whose intent and location can be masked. These and other points of concern continue to make information or cyber deterrence a concept that is continually controversial and a point of discussion.

This article focuses on how China views the information or cyber deterrence concept.[210] It is important to study China's and other nations' concepts to see if there is an evolving answer to the problem of defining and utilizing the term that other countries can utilize. Further, it is important to understand the context from which nation's make their assessments, as some nations are still developing their cyber deterrence concepts, while others are nearing the stage of completion. The conclusions focus on what the Chinese model reveals for the concept of deterrence in general. It appears that the Chinese intend to utilize the concept to achieve flexibility in negotiations and gain a psychological and digital strategic advantage, perhaps through a show of force. It is not clear whether the Chinese concept offers a better way of thinking about the term, however.

Cyber Deterrence versus Nuclear Deterrence

There are significant differences among nations regarding information/cyber

[210] The terms "information deterrence" and "cyber deterrence" are used interchangeably in this article. Both terms seem to be in use in China today.

deterrence and nuclear concepts. Of primary significance is just the construction, transport, and delivery issue. For nuclear weapons, a host of measures are required for each step of the process. Remaining covert during each step is extremely difficult. The construction, transport, and delivery issues are of more concern in the information/cyber concept due to difficulties in envisioning them. A good algorithm writer with knowledge of an important network's landscape can do much damage surreptitiously.

Another difference involves the pain and destruction associated with the attack. The pain that a nuclear explosion imparts is well-known. We can watch videos of blasts and predict destruction and fall-out impacts. An attack on underwater cables would not generate the type of panic that a mushroom cloud would produce. The pain of an information/cyber attack is less predictable. In the final analysis, social chaos and psychological fear may be the immediate fall-outs that most expect. A cyber attack on a banking system could produce panic overnight. What is less known are the effects of an attack on a digital decision-making apparatus, on an industrial or electrical infrastructure in winter, or on a communications satellite. Thus, for the immediate future the two types of deterrence cannot be equated, as one absolutely negates the use of the weapon (nuclear), while the other (cyber attacks) occur daily in a much more limited form (usually reconnaissance, although some attacks have caused harm).

Nuclear deterrence has a history and there has been ample time to discuss the issue. The advent and development of an information/cyber deterrence history, associated with technology, is shorter and advancements have been extraordinarily fast. In the past fifteen years we have witnessed the development of thumb drives, Facebook, YouTube, and numerous other online progress. Quantum computing is waiting in the wings. Cyber advancements mandate the development of new ways to consider deterrence beyond the term's nuclear heritage (or even the exclusion of cyber deterrence as a concept). New concepts could include, for example, ways to deter algorithm attacks on networks.

Under the umbrella of nuclear deterrence only governments or nation-states played. Under an information/cyber deterrence standoff, anyone can potentially play. No longer are we tied to governments and ambassadors and foreign ministries as the negotiators of nuclear deterrence. The cyber world operates in stark contrast to the nuclear one as extremists and terrorists see opportunities to play on the cyber field as well, which the nuclear era has not offered to date. With nuclear weapons we usually knew who the opponent was. With information/cyber issues, we do not always know. In short, it is time to talk about what we really mean by

information deterrence separate from the nuclear heritage of the term "deterrence." The information/cyber age has distinctive characteristics that we must work with in the future.

Yet another issue involves the legal aspect of nuclear versus information/cyber deterrence. Entire treaties and policies have already been developed to contain the proliferation and use of nuclear weapons. The construction of a similar system for information/cyber deterrence issues remains distant but the work of a host of legal experts has provided hope, such as the *Tallinn Manual on the International Law Applicable to Cyber Warfare.* The issue is still in need of final policy statements from a host of nations, however, as each nation fears being constrained by issues they could not foresee based on a lack of practical experience in the area.

Cyber Deterrence and China

Deterrence from a Chinese perspective emphasizes the use of psychological pressure or threats against an opponent. The psychological quality of deterrence appears to allow the PLA to use the cyber option so daringly in head-to-head confrontations based on risk and reward. In On China, Dr. Henry Kissinger noted Mao's tendency to utilize the psychological quality of deterrence:

> For Mao, the Western concept of deterrence was too passive. He rejected a posture in which China was obliged to wait for an attack. Wherever possible, he strove for the initiative. On one level, this was similar to the Western concept of preemption—anticipating an attack by launching the first blow. But in the Western doctrine, preemption seeks victory and a military advantage. Mao's approach to preemption differed in the extraordinary attention he paid to psychological elements. His motivating force was to … change the psychological balance, not so much to defeat the enemy as to alter his calculus of risks.[211]

When referencing a discussion with former paramount leader of China Deng Xiaoping, Kissinger noted that Deng had proposed a preemptive policy with regard to countering any offensive moves along China's borders that could be made by the then Soviet Union. Kissinger added that Deng's policy of preemption was an aspect of China's offensive deterrence doctrine.[212]

Today, it is unknown how closely China's cyber activities follow Deng's advice, that is, whether they are designed to develop an offensive preemptive cyber strategic advantage in anticipation of other nation's cyber capabilities. The continuous and

[211] Kissinger, p. 133.

[212] Kissinger, p. 364.

wide-ranging reconnaissance activities of the Chinese do, however, lead one to think that Deng's guidance is under consideration. Perhaps of greater importance is whether the PLA can make an opponent's cyber battlefield transparent or whether the PLA can generate new cyber combat power. This combination seems to offer a better chance of attaining a psychological advantage and information deterrence capability than old thinking about deterrence. An opponent will be deterred in the contemporary age when his risk calculus becomes problematic as a result of being confronted by an opponent with an offensive and deep reconnaissance capability that provides a seemingly all-knowing information picture that mirrors reality. These capabilities can even allow a force to "win victory before the first battle."

Over the past decade the Chinese have discussed the information/cyber deterrence concept in their books and journals. Writing in *China Military Science* in 2001, Zhao Xijun, a deputy commander of Second Artillery (responsible for nuclear weapons), defined deterrence as "military actions in the form of a show of force between countries or political groups, or an indication of their resolve and readiness to use force, intended to make an opponent not dare to take hostile action or to escalate his actions."[213] If one were to attempt to extrapolate what China's cyber deterrence theory might look like, Zhao's article is an interesting contemporary start point.[214] In this case, a show of force could simply be a digital presentation of another side's cyber capability.

Zhao bases deterrence theory to a degree on a combination of stratagems. Zhao notes that key factors in Sun Tzu's writings that influence contemporary deterrence theory include having superior military power, being fully prepared for war, having severe measures of punishment at one's disposal, having superb skill at "attacking strategy" and "attacking diplomacy," and making one's ideology of deterrence a lynchpin in a more complete system. All of these factors have cyber-age relevance. Zhao adds that a counter deterrent capability is the most effective method to stop the aggressive attempts of powerful nations from harming China's national interests.[215]

Zhao states it is necessary to combine truth with falsehood, a direct application of a stratagem. This combination can work to awe an enemy force into submission through the use of psychological means. Friendly (Chinese) forces must look for opportunities to attack an enemy force's power and resolve, thereby depriving an

[213] Zhao Xijun, "Victory without War and Modern Deterrence Strategy," China Military Science, 2001, pp. 55-60.

[214] Ibid.

[215] Ibid.

enemy of will power. When striking, they must do so resolutely, threatening targets with the greatest strategic value first. When there is no smoke or gunpowder, strategy and psychology act as multipliers of power and resolve in deterrence.[216]

A proper deterrence strategy includes the ability to judge the hour and to size up the situation while cautiously making decisions. A nation must have a good grasp of the target and the objective of its deterrent posture,[217] items that can be accomplished via digital reconnaissance. Zhao adds that China should use an integrated deterrence approach. A single deterrent force is not sufficient to constitute effective deterrence. Comprehensive power must be employed to retain the strategic initiative. This thought brings to mind the work of Qiao Liang and Wang Xiangsui in their book, *Unrestricted Warfare* The latter authors noted twenty-four different types of warfare and then theorized that a "tasty cocktail" mixture of the methods would best bring about success.[218] Thus, one might envision Zhao or others contemplating a cyber mixture of options that would serve as a deterrent force.

Editors Peng Guangqian and Yao Youzhi defined deterrence in their excellent 2001 work The Science of Military Strategy as "military conduct of a state or a political group in displaying force or showing the determination to use force to compel the enemy to submit to one's volition and to refrain from taking hostile actions or escalating the hostility."[219] Deterrence requires a deterrent force able to impact the overall strategic situation; the determination and volition to use the force; and the ability to make an opposing force perceive and believe these prior two points.[220]

The military action of strategic deterrence is defined as "the strategic move taken by a state or a political group for the purpose of forcing the opponent to submit to one's volition in the overall war situation through showing force or the determination of preparing to use force."[221] ." What strategic deterrence values most is momentum from military preparation, from showing a disposition of strength to an enemy, and from military strikes.[222] Thus, the creation of momentum, or shi, is a valued commodity of a deterrence concept or means of deterrence. Shi can also be

[216] Ibid.

[217] Ibid.

[218] Qiao Liang and Wang Xiangsui, Unrestricted Warfare, Pan American Publishing Company, Panama City, Panama, 2002, p. 118.

[219] Peng Guangqian and Yao Youzhi, editors, The Science of Military Strategy, English Edition, The Military Science Publishing House, 2001, p. 213.

[220] Ibid., pp. 213-214.

[221] Ibid., p. 222.

[222] Ibid.

interpreted as energy or strategic advantage. It is the latter concept that deterrence strives to attain whether through physical (force development and deployment) or mental (development of fear of retribution in an opponent).

Information deterrence is defined in *The Science of Military Strategy* as "the deterrence that depends on the powerful performance of information science and information technology, and it is put into effect by the momentum and power of information warfare."[223] In the world of information, the creation of deterrence from momentum is accomplished via the preparation of cyber power, showing an enemy force a disposition or capability of cyber strength, and from actual cyber strikes (perhaps the numerous computer reconnaissance activities of the Chinese).

Information deterrence, according to Peng and Yao, has the following features: first, permeability or the ability to permeate not only the military but also politics, the economy, culture, and science and technology; second, ambiguity, where the difference between information deterrence and information offense is hard to distinguish; third, diversity, such as unauthorized visits, malicious software, database disruption, etc.; fourth, two-way containment, where victims of an information attack may not be just the enemy but also others, to include oneself, due to the interconnectedness of networks and the global grid; and finally, the use of People's War as a capability, that is, the potential of people joining in to combat an enemy on the net.[224]

The Science of Military Strategy also notes the following points which apply more to the transmission of information ("information transmission is the necessary condition for creating the deterrent impact of strength and determination"[225]) in order to impact the cognition of an opponent:

> Deterrence requires turning the strength and the determination of using strength into information transmitted to an opponent, and to impact directly on his mentality in creating a psychological pressure to shock and awe the opponent…for this reason, effective strategic deterrence depends not only on strength and determination, but also on the above-mentioned information acquired by the deterred

[223] Ibid., p. 220. In a glossary at the back of the English language translation of The Science of Military Strategy, a translation the Chinese themselves provided, the term cyber is equated to the term informationization. That is, the same Chinese symbol was translated as "cyber, informationization." For that reason, this author sees little difference in cyber deterrence and information deterrence. The terms are used interchangeably hereafter.

[224] Ibid., pp. 220-221.

[225] Ibid., p. 215.

> side. If the opponent has not acquired the above information or the information acquired is not accurate, or the deterred side believes that the acquired information is only bluffing and intimidation, then it cannot create creditable and effective strategic deterrence…only when the opponent on receiving deterrence information perceives and believes that if he acts rashly, he may suffer a more severe punishment, can the deterrence obtain the expected impact.[226]

Finally, Peng and Yao write that deterrence seeks momentum in several postures: creating momentum through military preparation, demonstrating momentum by showing one's disposition of strength, and augmenting momentum with military strikes.[227]

In 2003 editor Cai Cuihong's book, *Information Networks and International Politics,* proposed an information deterrence theory. The work views the information umbrella as more utilitarian than the nuclear umbrella. An information umbrella can theoretically enable one side to see the adversary, while not allowing the adversary to see friendly activities. Control over information has become a new deterrent force as a result. Cai's work notes that "the side that controls information can manipulate the start and conclusion of wars, can use informatized weapons to paralyze enemy weapons and command systems, and can destroy the enemy's precision-guided weapons."[228]

Network warfare includes network spy warfare and network attack and defense warfare. It is a form of fighting similar to IW.[229] Network warfare could be conducted between countries, between countries and organizations, between countries and individuals, between organizations, between organizations and individuals, and even between individuals.[230] The deterrent strength of China's armed forces will be balanced on the basis of its computing power, communications capacity and reliability, real-time reconnaissance capabilities, computer simulation capabilities, and other information elements. These elements can deter through preying on an opponent's misconceptions and administering psychological pressure,[231] accomplished through information control. Cai added the more

[226] Ibid., pp. 214-215.

[227] Ibid., p. 222.

[228] Cai Cuihong, Information Networks and International Politics, [publisher unknown], 2003, pp. 163-164.

[229] Ibid., p. 173.

[230] Ibid., p. 176-177.

[231] Ibid., p. 178.

uncomfortable assessment that "information network warfare under conditions of nuclear deterrence will be the new form of future international conflict."[232]

In 2004, the journal *China Military Science* published a few articles on strategic deterrence that offer insights into how it could be applied to cyber issues. Zhou Peng and Wen Enbin, from the Academy of Military Science, wrote that strategic deterrence refers to a "country or political bloc's military actions to compel an adversary to not dare take hostile action or escalate actions through a show of force or indicating the resolve of being prepared to use force, thereby achieving specific strategic goals."[233] The possession of military strength is a prerequisite, along with the resolve to use force and the ability to make the target of deterrence aware of one's capabilities. Targeted deterrence can be achieved based on the controllability and flexibility of informatized measures.[234] Thus a show of force could be presented to another country in the cyber age simply by demonstrating control over a network.

According to Zhou and Wen, former Chinese President Jiang Zemin recommended elevating deterrence to the level of strategy. The concept of strategic deterrence could be used to contain war, delay its outbreak, or prevent its escalation. The core of new deterrence capabilities should be "assassin's mace" technologies. Jiang emphasized mobilization measures as a priority development. China has emphasized information mobilization processes ever since, with many such military and civilian exercises conducted annually. China "must establish an emergency mobilization combat force" due to the fast nature of high-tech wars and corresponding requirement to be ready at a moment's notice. A war's start can have decisive significance in the information age. Mobilization capabilities enable China to unleash the deterrent effect of people's war under high-tech conditions.[235] This emergency mobilization force could be the cyber militias that China has developed or a host of other cyber elements.

Comprehensive national strength, in Zhou's and Wen's opinion, generates a reliable deterrent effect that must be developed now during China's so-called 20-year "window of strategic opportunity." A good deterrent force involves the use of nuclear deterrence, conventional deterrence, space deterrence, and information deterrence, again reminding one of cocktail warfare[236] The authors add that "The acme of the art of strategic guidance is fully reflected in the proper selection and

[232] Ibid., p. 172.

[233] Zhou Peng and Wen Enbin, "Developing a Strategic Deterrence Theory with Chinese Characteristics," China Military Science, No. 4 2004, pp. 19-26.

[234] Ibid., pp. 20-21.

[235] Ibid., pp. 22-23.

[236] Ibid., pp. 24-25.

constant innovation of deterrence forms; it is the most real, most dynamic part of wielding strategic deterrence."[237]

In a second 2004 *China Military Science* article, a research group from the Academy of Military Science (AMS) wrote an article on strategic deterrence. They noted that to deter, a nation must possess an adequate force, the determination to use the force, and the ability to make an opponent believe that these conditions exist.[238] Accusations from a host of nations accusing China of extended cyber reconnaissance activities inside commercial firms worldwide indicate they could be in the process of establishing this type of deterrent form.

The AMS research group stated that a combination of nuclear, conventional, space, people's war, and information deterrence was needed to offer a comprehensive deterrent. The latter element was of particular importance. It permeates each of the other forms of deterrence and offers both psychological ambiguity and the diversity of using either hard or soft kills. What strategic deterrence values most, the authors noted, is momentum created by military preparation, a demonstration of the disposition of strength to an opponent, and the ability to augment momentum with military strikes.[239] China has demonstrated it preparation of an informatized military, has demonstrated its suspected ability to penetrate foreign systems, and has continued to upgrade its military force.

In 2007 Major General Li Deyi stated that information deterrence will rise to a strategic level close behind nuclear deterrence. New and important modes of deterrence will include information-technology deterrence, information-weaponry deterrence, and information-resource deterrence. Further, counter information deterrence will be part of China's new mode of thinking.[240] Also in 2007 Senior Colonel Deng Yifei wrote that information deterrence would be a means, behind nuclear deterrence, to achieve national strategic goals and military strategic goals. Deng believes that information has become the core concept in military thinking. Vying for information supremacy and forming information deterrence capabilities are the key areas of current military thought in his opinion.[241]

---

[237] Ibid., p. 25.

[238] Academy of Military Science Research Group, "Strategic Deterrence," China Military Science, No. 5 2004, pp. 143-156.

[239] Ibid.

[240] Li Deyi, "A Study of the Basic Characteristics of the Modes of Thinking in Informatized Warfare," China Military Science, No. 4 2007, pp. 101-105.

[241] Deng Yifei, "A Revolution in Military Thinking in the Information Age," China Military Science, No. 6 2007, pp. 71-78.

In 2009 a few top nuclear generals in China wrote how information resources and the information components of weaponry apply to information deterrence. Zhou Fangyin noted that the concept of information deterrence is defined as forcing an adversary to lay down his weapons through demonstrations or through highlighting friendly force weaponry's advanced precision under informatized conditions.[242] Zhou's example leads the reader to believe he is talking more about precision guided weaponry, of course, than cyber attacks on infrastructure.

In 2010 Senior Colonel Yao Yunzhu, writing in the US journal *Air & Space Power* stated that China will continue to apply deterrence at the grand strategic level while depending more on "uncertainty" for a better deterrence effect.[243] Even though her comments were with regard to nuclear deterrence, they could easily fit an information deterrence scenario. In the age of computer hacking, "uncertainty" as to a hacker's actual identity or government connection is perhaps the concepts biggest obstacle for those attacked or reconnoitered to overcome.

Also in 2010 Chinese analysts Tang Lan and Zhang Xin, at a US conference hosted by the East West Institute, delivered a paper titled "Can Cyber Deterrence Work?" The authors wrote that the anonymity, global reach, scattered nature, and interconnectedness of networks and the Internet reduces the efficacy of cyber deterrence and can even "render it completely useless."[244] These issues further separate cyber deterrence from deterrence issues associated with nuclear issues, not to mention that cyber attacks are associated with low-cost and low-risk issues in comparison to nuclear ones. Tang and Zhang noted that "indirect damage is the primary problem with cyber deterrence."[245] They added the following points: mutual assured destruction does not apply to cyber deterrence; major obstacles to cyber deterrence are difficult technical hurdles, a lack of social responsibility and security awareness, and inadequate international cooperation (especially the reluctance of states to "budge on their perceived cyberspace interests or on differences they have in terms of laws and politics"), and the lack of a clear stance on what constitutes illegal and harmful information based on different beliefs in the free spread of information or other customs and traditions.[246] Thus these authors stressed the concept's ineptitude to deal with contemporary technical issues.

---

[242] Zhou Fangyin, "The Effect of the Information Revolution on Military Affairs and Security," Beijing Xiandai Guoji Guanxi, 1 August 2001, pp. 28-32.

[243] Yao Yunzhu, "China's Perspective on Nuclear Deterrence," Air & Space Power Journal, Spring 2011, p. 30.

[244] Tang Lan and Zhang Xin (edited by Andrew Nagorski), "Can Cyber Deterrence Work?" East West Institute Conference, April 2010, p. 1.

[245] Ibid.

[246] Ibid., p. 2.

The Chinese media did carry several articles in 2011 on information/cyber deterrence. One article in the authoritative *China Military Science* noted that China's core military capability was based on the ability to win local wars under informatized conditions. This capability is supported by the power of deterrence. Authors Liu Yongming and Jin Zhenxing noted the following with regard to China's information offensive and defensive capabilities in the article:

> This includes the capability of effectively conducting **strategic information deterrence**; the capability of detecting, infiltrating and damaging, and controlling information nodes of hostile operation systems; the capability of dealing hard destruction to hostile information systems; the capability of launching network attacks on hostile computer networks; the capability of guarding against hostile information reconnaissance; the capability of resisting hostile information interference; and the capability of rebuilding information systems.[247]

Many of the articles in 2011 discussed the US cyber strategy that was published at that time. The comments were highly negative in regard to the utility of the US use of a cyber deterrence concept. One of those articles noted the following about a supposed US reliance on cyber deterrence in future wars:

> The idea of so-called 'cyber deterrence' proposed by senior US military officials is more or less the same as the 'nuclear deterrence' proposed in the past…With regard to the United States, 'cyber deterrence' can be composed of three parts: First, a cyber army capable of both defense and offense; second, development of weapons including 'digital bombs' used in cyber attacks; and third, when necessary, the use of real military force to attack the enemy's network. It will be impossible for the United States or a small number of nations to monopolize the three component parts as the first two can be achieved even in individual behavior and can be easily imitated.[248]

Another anti-US 2011 article noted that "the effectiveness of cyber deterrence is questionable because of the specificity, complexity, and uncertainty of cyber technologies. Moreover, deterrence theory has exacerbated the distrust

[247] Liu Yongming and Jin Zhenxing, "Study on Hu Jintao's Important Instructions on Enhancing Capabilities of Accomplishing Diversified Military Tasks with Winning Local Wars under Informatized Conditions as the Core," China Military Science, No. 6 2011, pp. 1-9.

[248] Yu Xiaoqiu, "Cyber Deterrence Is a Dangerous Game," Renmin Ribao Online, 25 July 2011, p. 3.

and insecurity among countries and thus hindered international cooperation in cyberspace."[249]

In 2012 and into 2013 Chinese articles appeared to distance themselves from the information/cyber deterrence concept. Instead, deterrence was linked with "winning local wars under informatized conditions." For example, an article describing the opening of the first session in 2013 of the 12th National People's Congress noted that "deterrence and actual-combat capabilities under informatized conditions further strengthened" in 2012.[250] Senior Colonel Xu Weidi, writing in 2012 on military deterrence for the US's *Air and Space Power Journal,* noted the following in his article:

> In other words, during the entire Cold War Era, while the Western powers talked about deterrence, they often exercised coercion. This twisted and alienated 'deterrence' is best demonstrated by what they did with forward defense—a defensive posture in which one claims defense by 'pointing his bayonet right at the neck of the opponent.'[251]

The concept of coercion was cited as applying to Chinese thought as well, however. In an article by Dean Cheng, a US expert on the Chinese military, it was noted that the *PLA Encyclopedia* defined a strategy of deterrence, or *weishe zhanlue*, as the "display of military power, or the threat of the use of military power, in order to compel an opponent to submit."[252] So it appears that the idea to compel or coerce is not foreign to the PLA's concept of deterrence. Some US analysts even translate the Chinese concept of deterrence as coercion.

Conclusions: Have the Chinese Helped the Discussion?

Key points to take away from the discussion above are as follows:

- Deterrence can be defined as military actions in the form of a show of force.
- When there is no smoke or gunpowder, strategy and psychology act as multipliers of power and resolve in deterrence.

---

[249] Unattributed article, "Reality of the Virtual World," China Daily Online (in English), 16 July 2011.

[250] Unattributed article, "Rally Wisdom and Forces to Hold Up the 'China Dream,'" Jiefangjun Bao Online, 5 March 2013, p. 1.

[251] Xu Weidi, "Embracing the Moon in the Sky or Fishing the Moon in the Water?" Air & Space Power Journal, July-August 2012, p. 16.

[252] Dean Cheng, "Chinese Views on Deterrence," Joint Force Quarterly, Issue 60, First Quarter, 2011, p. 92.

• New and important modes of deterrence will include information-technology deterrence, information-weaponry deterrence, and information-resource deterrence. Information deterrence will rise to a strategic level close behind nuclear deterrence, a way to achieve national and military strategic goals.

• A good deterrent force involves the use of nuclear deterrence, conventional deterrence, space deterrence, and information deterrence, again reminding one of cocktail warfare.

• The side that controls information can manipulate the start and conclusion of wars, can use informatized weapons to paralyze enemy weapons and command systems, and can destroy the enemy's precision-guided weapons.

• The deterrent strength of China's armed forces will be balanced on the basis of its computing power, communications capacity and reliability, real-time reconnaissance capabilities, computer simulation capabilities, and other information elements. These elements can deter through preying on an opponent's misconceptions and psychological pressure,

• Strategic deterrence refers to a "country or political bloc's military actions to compel an adversary to not dare take hostile action or escalate actions through a show of force or indicating the resolve of being prepared to use force, thereby achieving specific strategic goals."

• An opponent will be deterred when his risk calculus becomes problematic as a result of being confronted with an opponent with an offensive and seemingly all-knowing information image that appears realistic.

• Today, it is unknown how closely China's cyber activities will follow paramount leader Deng Xiaoping's advice from the 1990s, that is, whether they are designed to develop a preemptive cyber strategic advantage to counter another nation's potential offensive moves.

Several items from this list are valuable for understanding China's cyber deterrence concept. First is China's focus on the use of strategy and psychology in its application of deterrence theory. This focus reflects China's long held interest in these two topical areas. Other nations must assess this contextual perspective as they attempt to understand the Chinese approach to cyber deterrence, to include what terms mean and how they will affect China's risk calculus. Second, it appears China views the contemporary deterrence situation as dependent on the integration of various types and modes of deterrence such as space, conventional, and information, eventually resulting in the achievement of strategic deterrence. This integration of concepts has been advanced as early as 1999, albeit with other ways

to fight wars in mind. Third, China believes that deterrence's strength is enhanced through the measurement of computing power, information reliability, and other factors. These factors may be considered and computed according to some internal formula in China such as the assessment of comprehensive national power. Fourth, just like with other forms of deterrence, China understands that cyber deterrence must be able to demonstrate an adequate digital show of force that it can use to intimidate or deter others when required. Such a show of force could even be the digital exposure of pirated secrets, such as occurred during the Wiki leaks fiasco. Finally, Chinese authors believe the nation must be able to demonstrate control over information if it is to maintain stability over its digits and manipulate successfully the start and finish of a cyber deterrence-type scenario. While all of these points are well taken, articles in 2011 demonstrated that there is a negative perception of cyber deterrence in China when linked with US cyber strategy. The deterrence concept is palatable to the Chinese, however, when associated with winning local wars under informatized conditions.

Overall, Chinese theorists offered several areas of thought for other nations to consider in the development of a cyber deterrence concept. The essence of China's deterrence practice appears to be resolving war with non-war measures and applying stratagems such as win without fighting and win victory before the first battle. Chinese style cyber deterrence is of a strategic nature and discussion among Chinese experts indicates that various types of cyber or information deterrence conditions are under consideration. Further, Chinese theorists understand that, due to the fast nature of high-tech wars, a war's start can have decisive significance. For that reason China "must establish an emergency mobilization combat force" if it is to immediately unleash the deterrent effect of people's war under high-tech conditions on an opponent. The Chinese add that they must prepare cyber counter-deterrents to any potential opponent's actions. This might involve using military exercises to demonstrate strength in the use of technologies or perhaps even an announced reconnaissance activity to prove or intimate that an opponent is impotent to stop them.

In summary, China has been discussing a strategic information/cyber deterrence policy that will keep other nations guessing, which deterrence policies are designed to do. This policy is based, as with nuclear issues, on the idea of uncertainty in order to achieve a better deterrent effect. China's context is different than that of either the US or Russia, and must be taken into consideration when other nations assess China's final goals and rationale for contemplating the use of the concept. The concept appears to be a way for the PLA to preserve combat power and control over military, sovereignty, and economic issues. The Chinese approach

has, however, been helpful in providing other nations a varied perspective or way to consider deterrence. A most important remains to avoid conflict. The PLA apparently hopes that a strong cyber deterrence policy will help assist the country to find the time and budget to achieve the military aspect of the "China Dream" of new President Xi Jinping.

DISCLAIMER: The views expressed in this report are those of the author and do not necessarily represent the official policy or position of the Department of the Army, Department of Defense, or the U.S. government.

The Foreign Military Studies Office (FMSO) assesses regional military and security issues through open-source media and direct engagement with foreign military and security specialists to advise army leadership on issues of policy and planning critical to the U.S. Army and the wider military community.

Йоко Нитта
(Yoko Nitta)
Исследовательский институт
науки и технологий для общества,
Японское агентство по науке и технологиям

ПОДХОДЫ ЯПОНИИ К КИБЕРБЕЗОПАСНОСТИ

В XV веке Фрэнсис Бэкон сказал: «Scientia potestas est» («Знание есть сила»). Однако согласно Элвину Тоффлеру в средние века главным орудием власти была сила физическая: правящая элита, пользуясь своим могуществом, грозила расправой всем непокорным. В ходе промышленной революции власть перешла к торговцам, завладевшим важными ресурсами и каналами сбыта. Таким образом, физическая сила привела к обогащению.

В наше время, в эпоху Третьей волны, сила знания приходит на смену богатству в качестве основного источника власти. Обладая нужными знаниями, можно добиться многого, не прибегая к использованию материальных ресурсов. Мы с вами – свидетели перехода правления к образованной элите (и народным массам). Наш мир все больше ориентируется на технологии. Эволюция власти пошла по новому пути, и Интернет превратился в мощнейший рычаг управления. Информационные и коммуникационные технологии стали главным стимулом экономического роста. Мировому сообществу необходимо осознать, что сейчас происходит сдвиг парадигмы структурных изменений. Приходит время больших данных, и мир уже вступил в эпоху «Интернета вещей». В нашей повседневной жизни возникла новая угроза – угроза кибератаки, и согласно отчету FireEye в первой половине 2012 года число энергосбытовых и коммунальных предприятий, подвергшихся атакам с использованием современных вредоносных программ, выросло на 60 %.

Мир переходит от связности к гиперсвязности, и это, несомненно, оказывает определенное влияние на трудовую деятельность, экономику и образо-

вание. Весной этого года президент Европейского совета Херман Ван Ромпёй в одной из своих речей раскрыл перспективы развития кибертерроризма, подчеркнув, что кибератаки могут поставить под угрозу безопасность таких важнейших артерий современной жизни, как телекоммуникации, банковские системы, аэропорты и сети энергоснабжения. Президент США вскоре после вступления в должность призвал общество всесторонне пересмотреть вопросы безопасности и возможности восстановления всемирной цифровой инфраструктуры и поставил эту задачу перед своей администрацией в качестве первоочередной. В ООН обсуждается вопрос необходимости установления доверительных отношений между союзниками в области международной информационной безопасности.

Согласно определению Федерального агентства США по управлению в чрезвычайных ситуациях, кибербезопасность – это «защита информации и имущества от кражи, порчи или стихийных бедствий, при которой законные пользователи по-прежнему имеют доступ к таким информации и имуществу и могут пользоваться ими». Одно это определение свидетельствует об огромном значении информационных систем и данных, которые мы пересылаем и храним с их помощью. Именно поэтому коммуникационная и информационная инфраструктура подвергается такому же природному и антропогенному риску, как и физическая инфраструктура (здания, дамбы, сети энергоснабжения). Причинами антропогенных происшествий, происходящих ввиду действий или бездействия людей, обычно являются человеческие ошибки, халатность, преступные и другие действия. Стихийные бедствия происходят не по злому умыслу и не из-за ошибки оператора, но и они, тем не менее, способны нанести аналогичный – и даже больший – ущерб информационной инфраструктуре (от ограничения функциональности до полного разрушения).

В последнее время мы часто слышим о том, что постоянные атаки на национальные институты, предприятия военно-промышленного комплекса, коммерческие организации и научно-исследовательские институты с применением современных средств могут привести к раскрытию государственной тайны и секретной технологической информации.

Два основных аспекта, которые рассматриваются в «Таллинском руководстве», – это «*jus ad bellum*» (право войны) и «*jus in bello*» (международное гуманитарное право). Однако по утверждению Атлантического совета НАТО, «*“Таллинское руководство” рассматривает только “букву закона”, т. е. пытается использовать существующие законодательные нормы права, и не дает рекомендаций по его практическому применению в конкретных случаях. Следующий*

шаг в этом направлении станет возможным только благодаря действиям политиков, заключению новых международных договоров и рассмотрению новых судебных прецедентов». Страны мира ведут переговоры по разработке совместной стратегии и политики с целью решения вопросов кибербезопасности с точки зрения национальной безопасности и экономического роста. Обеспечение безопасности киберпространства стало вопросом общемирового значения, который рассматривается с глобальной точки зрения. В то же время разные государства трактуют кибербезопасность по-разному. Как подчеркивает Европейское агентство по сетевой и информационной безопасности, единое исчерпывающее определение этого термина на уровне ЕС и международном уровне отсутствует.

Япония не является исключением. Ее национальная безопасность также находится под угрозой. Сфера безопасности переживает переходный период, поэтому наша нация уязвима и подвержена преступному влиянию. В чем же причина нависшей над нами угрозы? В свободном обмене информацией? Этот вопрос выходит за рамки национальной безопасности и затрагивает также политическую, экономическую и социальную сферы.

Он касается отдельных граждан, сообществ и всего государства в целом и имеет множество различных, но неразрывно связанных между собой аспектов. В последнее время среди японцев стало популярным носить талисманы, которые должны защищать личные устройства от вирусов.

Сейчас в Японии существуют следующие проблемы:

- Направленные кибератаки (объектами таких атак являются определенные организации, включая предприятия малого и среднего бизнеса, государственные службы и крупные компании)

- Как определить, может ли наша нация реализовать свое право на индивидуальную или коллективную самооборону или на привлечение вооруженных сил в качестве меры противодействия информационному нападению со стороны другого государства? Японское правительство приняло закон об обеспечении национальной безопасности в чрезвычайных условиях, но вопросы кибербезопасности в него включены не были. Вооруженные силы Японии имеют право оказывать сопротивление только в случае вооруженного нападения. Проблема состоит в том, что правительство не определило, какие именно кибератаки можно считать вооруженным нападением.

- Государство не может заблокировать коммуникационный канал даже при наличии вредоносного ПО, так как это будет являться прямым нарушением права на тайну связи, прописанного в конституции.

- Нехватка человеческих и технологических ресурсов для отражения кибератаки.

Япония пока не в состоянии самостоятельно проводить криптоанализ (анализ) вирусов и полностью зависит в этом плане от других государств.

- Структура командования недоработана и в случае информационного нападения может оказаться неэффективной. В Японии есть Национальный центр по информационной безопасности, который должен инициировать ответные действия в случае возникновения угрозы.

При этом наблюдается острая нехватка специалистов, которые на практике были бы способны оказать необходимое противодействие.

- Между министерствами наблюдается расхождение во мнениях касательно вопросов кибербезопасности, они не готовы идти на сотрудничество и делиться друг с другом имеющимися данными.

- Необходимо, чтобы граждане также осознали сложившуюся ситуацию. В повседневной жизни большинство японцев не уделяет проблеме информационной безопасности достаточного внимания.

В апреле 2005 года в Японии при Секретариате Кабинета министров был сформирован Национальный центр по информационной безопасности (НЦИБ), в задачи которого входит координирование действий по повышению уровня безопасности как в рамках сектора внутренней безопасности, так и на межсекторальном уровне. Кроме того, регулярно проводятся конференции по информационным сетям и сетям связи, целью которых является усовершенствование стандарта информационной безопасности для государства и важнейших предприятий национальной инфраструктуры, а также наращивание ресурсов для противодействия кибератакам. НЦИБ был основан после совершения анонимного кибернападения на японское правительство в 2005 году.

В феврале 2013 года японский премьер-министр Синдзо Абэ в своем выступлении на 183-й сессии Парламента подчеркнул необходимость усиления ответных мер и расширения ресурсов для противодействия киберпреступлениям и кибератакам, направленным против определенных структур и угрожающим безопасному использованию Интернета.

Это привело к тому, что в марте 2013 года Главное управление полиции объявило о решении сформировать специализированное национальное полицейское подразделение штатной численностью 140 человек, которое будет бороться с киберпреступностью, и в том числе с внешней информационной агрессией. Отряды этой так называемой «киберполиции» планируется

расположить в Осаке, Токио и других стратегически важных районах. В состав отрядов входят специалисты, набранные из частных компаний, которые свободно владеют английским, китайским, корейским и русским языками. Основная задача киберполиции – вывести обеспечение безопасности государственных служб, подрядчиков Министерства обороны и частных операторов объектов национальной инфраструктуры на новый уровень.

Кроме того, в апреле 2013 года Министерство внутренних дел и коммуникаций Японии организовало Научно-исследовательский центр информационной безопасности, который займется разработкой технологий защиты от кибератак с использованием методов практического обнаружения. При помощи этого центра планируется решить следующие задачи: создание общей платформы для научно-исследовательских институтов кибербезопасности, которые станут центрами сосредоточения всех знаний и опыта нашей нации в этой области; разработка основных практических принципов противодействия новым киберугрозам; внедрение общественного опыта в новые разработки; а также расширение сотрудничества с Европой, Азией и США в области международной информационной безопасности. Такой подход позволит оптимизировать мониторинг информационных сетей и расширить возможности информационного анализа и составления заключений, однако окажется бесполезным при отсутствии обмена информацией и сотрудничества для разработки более решительных мер.

Для решения этой проблемы в мае 2013 года был составлен черновой вариант Стратегии информационной безопасности, который сейчас выставлен на публичное обсуждение. Суть этой стратегии заключается в следующем. Обстановка в сфере информационной безопасности стремительно изменяется. В первую очередь Японии необходимо согласовать действия различных министерств. За последние три года уровень риска, которому подвергается Интернет-пространство, растет и расширяется невероятными темпами и достиг мирового уровня. Увеличиваются размер и масштаб киберугрозы.

Киберпространство стало основной площадкой для проведения многих повседневных социальных, экономических и административных операций. Объединение и интеграция в этой области значительно ускорились.

Киберпространство стало неотъемлемой частью жизни нашей нации. Оно способствует решению социальных проблем и обладает огромным потенциалом в плане экономического роста и инновационной деятельности, мировое сообщество считает его стимулом развития и, несомненно, продолжит его осваивать. Ввиду этого, кибератаки на информационную ин-

фраструктуру превратились в реальную угрозу и стали одной из первоочередных проблем национальной безопасности и управления риском. Япония претендует на звание одного из наиболее развитых информационных государств мира, и чтобы сохранить свою репутацию, ей необходимо обеспечить достойный уровень кибербезопасности. Стремительно расширяется диапазон групп, подвергающихся кибератакам (от частных лиц и отдельных семей до комплексных предприятий социальной инфраструктуры). Несмотря на все усилия японского правительства, увеличивается риск информационного нападения. Этот риск затрагивает такие сферы, как национальная безопасность, управление риском и конкурентоспособность нашей страны и является предметом постоянного беспокойства для наших граждан.

Стратегия информационной безопасности была разработана для создания информационно защищенной нации. В рамках этой стратегии можно выделить следующие четыре основные цели: обеспечение свободного и безопасного обмена информацией; попытка вывести проблему кибербезопасности на более высокий уровень; оптимизация ответных действий, направленных на решение этой проблемы; разработка плана действий и упрочение сотрудничества на основании принципов социальной ответственности. В стратегии также четко определены роли всех заинтересованных сторон (государства, предприятий инфраструктуры, коммерческих организаций (научно-исследовательских институтов), отдельных пользователей и компаний, осуществляющих операции через Интернет).

Было определено три основных целевых направления работ, которые необходимо выполнить до 2015 года. Планируется, что правительство обеспечит надежность и устойчивость киберпространства, повысив уровень информационной безопасности и обеспечив защиту от кибернападений; создаст новые структуры, способствующие динамичному развитию киберпространства, нацеленные на стимулирование научно-исследовательской деятельности, привлечение на конкурентной основе новых кадров для обеспечения кибербезопасности и просвещение граждан по вопросам кибербезопасности; и сформулирует задачи в отношении киберпространства, основываясь на дипломатических принципах, глобальном освоении этого пространства и международном сотрудничестве.

Развитие киберпространства в Японии поручено НЦИБ. Перед ним поставлены такие задачи, как формирование системы для экспертов по кибербезопасности и реорганизация в «Центр кибербезопасности» до 2015 года.

Представляется необходимым рассмотреть следующие нормативные аспекты для решения проблемы кибербезопасности в Японии:

- Управление общим достоянием человечества;

- Коренное преобразование архитектуры систем безопасности;

- Информированность граждан;

- Совместная стратегия.

Управление общим достоянием (признание исключительности человечества):

• Обеспечение стабильности на основании существующих норм международного права (режим управления);

• Сохранение доверия стратегических партнеров;

• Отсутствие конфликтов (мирное использование ресурсов);

• Создание единой международной платформы;

• Установление стабильных и мирных отношений в международном сообществе;

• Содействие осознанию международной ответственности (в соответствии с идеологией мирового гражданства);

• Критическое мышление;

• Обсуждение этических вопросов;

• Ответственный подход к обязательству по преобразованию информации и знаний в интересах людей.

Стратегия зашиты от риска за счет привлечения незатронутых сторон:

• Косвенная защита: рассредоточение риска;

• Умеренные меры: привлечение незатронутых государств, формирование альянса и налаживание многоуровневого сотрудничества;

• Кардинальные меры: наращивание военного потенциала и развитие прочного сотрудничества с другими странами (характерно для традиционного подхода).

Изучение прецедентов:

• Формирование у граждан глобального подхода к проблеме;

• Глобальные пользователи: гиперсвязность сделает общество более раздробленным и уязвимым;

• Изучение исключительных прецедентов (и поиск решений) .

Здесь представляется целесообразным дать определение слову «глобальный».

Следующие рассуждения помогут нам лучше понять его смысл

Следует соблюдать осторожность при употреблении термина «глобальный». Каково традиционное международное понимание его значения? Посмотрите на современную политическую карту мира. Удивительно, насколько по-разному различные государства используют этот термин и что они в него вкладывают. Картина меняется в зависимости от того, из какого полушария мы смотрим на определенную страну. Необходимо учесть, как выглядит наша страна, готовая к отражению кибернападения, с точки зрения другого региона. Кроме того, при разработке политического курса следует принять во внимание точку зрения граждан (например, путем публичного обсуждения соответствующих документов). Должны ли мы выработать единую стратегию и издать «глобальный» нормативный документ, чтобы решить проблему кибербезопасности?

Люди понимают, что защита – это лишний повод для нападения, а взаимное недоверие делает их более уязвимыми, но ничего не могут с этим сделать, поскольку твердо уверены, что прагматический подход является основополагающим, в том числе и в вопросе кибербезопасности.

Сейчас, чтобы решить этот вопрос и проанализировать новый этап его развития, нам необходимо пересмотреть этический и философский аспекты. Эти аспекты – ключ к индивидуальности. Кроме того, для нового этапа развития важным также является аспект взаимодействия.

Поль Гоген задавался вопросом: «Откуда мы пришли? Кто мы? Куда мы идем?» Томас Джефферсон сказал: «Если между свободой и безопасностью народ выбирает безопасность, в конечном итоге он теряет и то, и другое».

Для Японии проблема кибербезопасности неразрывно связана с ее ролью суверенного, самостоятельного государства. Как Япония определяет границы своей ответственности в рамках альянса с США, который задает общий курс японской политики национальной безопасности? Следует ли Японии пересмотреть эти границы? Если да, то каким образом? Как Японии следует решать новые задачи, возникающие в связи с развитием информационных технологий?

Источники

- Фрэнсис Бэкон
- Элвин Тоффлер
- Отчет в рамках Стратегии кибербезопасности Японии, май 2013 г.
- Анализ угроз компании FireEye за 1-ю половину 2012 г.

• Стратегии национальной кибербезопасности: практическое руководство по разработке и исполнению, декабрь 2012 г.

• Financial Times, статья «Nations are chasing the illusion of sovereignty» («В погоне за мнимым суверенитетом»), 6 июня 2013 г.

http://www.ft.com/intl/cms/s/0/d1dcdb6a-cddb-11e2-a13e-00144feab7de.html#axzz2WqqIiyJz

• Financial Times, статья «Southeastern shift: The new leaders of global economic growth» («Юго-Восточная Азия – новый лидер по глобальному экономическому росту»)

• Интернет-издание Science News, «Japan police to launch national cyber crime force» («Японская полиция объявила о создании подразделения по борьбе с киберпреступностью»), 28 марта 2013 г.

• Таллиннское руководство о применимости международного права к киберконфликтам

http://www.ejiltalk.org/the-tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/

• Сайт Атлантического совета НАТО

http://www.acus.org/new_atlanticist/reason-finally-gets-voice-tallinn-manual-cyber-war-and-international-law

ОТКАЗ ОТ ОТВЕТСТВЕННОСТИ: В настоящем докладе автор предлагает собственный анализ ситуации, который может не совпадать с точкой зрения Исследовательского института науки и технологий для общества и Японского агентства по науке и технологиям.

Yoko Nitta
Associate Fellow
Research Institute of Science and Technology for Society (RISTEX),
Japan Science and Technology Agency

JAPAN APPROACHES TOWARDS CYBERSECURITY

Francis Bacon said scientia potestas est (knowledge is power) in 15C. Alvin Toffler indicates violence was the basic power of the nobility in ancient times, where a powerful elite worked largely through domination that threatened violence to those who did not comply. In the industrial revolution, as the merchant classes became more powerful and gained control of critical resources and channels , violence gave way to wealth.

Today, in the Third Wave, the power of knowledge is replacing commercial wealth as the primary source of power. If you have the right knowledge, you can get a lot done without recourse to money. Power is thus moving to the educated elite (and masses). We are now moving ahead to hard technology-oriented. Evolution of power has transformed and the internet is a great leverage of power in this regard. ITC is a driving force for economy growth. Now we should realize that we are in the middle of paradigm shift of fundamental structural change. Big data is almost here and the era called 'Internet of Things' has come. Cyber attack is a new threat to our daily life and energy and utility companies saw a 60% increase in advanced malware incidents in 1H 2012 according to Fire Eye report.

The world went from connected to hyper-connected and it gives a certain impact on job, industry and school. Herman Van Rompuy, President of European Council, made a speech this spring regarding perspective of cyber terrorism saying that it is a potential threat to the arteries of globalized modern life, telecommunication, banking systems and airports or energy grids. The U.S. President called for a comprehensive review of the security and resiliency of the global digital infrastructure, a top priority in his administration soon after taking office. United Nations has discussed to find the establish trust among alliances.

According to the US Federal Emergency Management Agency, cybersecurity is "the protection of information and property from theft, corruption, or natural disaster while allowing the information and property to remain accessible and productive to its intended users." This definition alone demonstrates the value of the involved systems and the data they transfer and store. Because of this value,

communications and information infrastructures are subject to the same man-made and natural threats, risks, and vulnerabilities as are physical infrastructure such as buildings, dams or power lines. Man-made events are generated by human actions or omissions stemming from human error, negligence, criminal behavior, or other motives. While natural disasters lack the intent or capability for operational error, they can have the same (or worse) results on cyber infrastructure, including damage ranging from inconvenience or degradation to outright destruction.

Lately it is pointed out that national institute, defense industries and infrastructure business and institute of research and development advanced persistent attack has threatened to exploit classified realm and technology information.

The Tallinn Manual's primary focus is the *jus ad bellum* (the law governing the use of force) and *jus in bello* bello (international humanitarian law). According to Atlantic Council, *'The Tallinn Manual is only an assessment of "black-letter law," which means it only tries to apply the law as it exists today; the book is silent on what the law should say on a topic. Only policymakers (and future treaties or court cases) can take that next step.'* Overseas countries develop cooperative strategies and policies to tackle cyber security form the point of view of national security and economic growth. Cyber space is already world- wide common challenge and with global view point. There is no common understanding towards cyber security and European Network and Information Security Agency(ENISA) points out that there is no comprehensive definition at EU level and at international level.

Japan is also under national security threats. Security is at transitional moment and is uncertain and exploitive. Is it growing ominous under information unbound? The context of this issue is not just national nuisance but so diverse, it is political, economic and social.

The players are individual, groups and state and it is entangled and intertwine. Nowadays lucky charms for 'IT protection' has been popular to carry with.

Here are current challenge case in Japan

- Targeted cyber attack (mainly on certain organization including SME, government and blue chip companies)

- How to define to invoke the right of (collective) defense or implement their right of Self Defense Force against cyber attack from overseas since although Japan put into effect emergency legislation on national security, cyber attach is not incorporated into this law. In Japan SDF is not allowed to invoke their right only at occurrence of an armed attack. The problem is Japan has not defined what situation should be regarded as armed attack in terms of cyber attack

- Japan cannot block communication even if there is dubious virus since it infringes on the constitutionally guaranteed secrecy of communication

- Lack of resources (human/ technology) to deal with cyber attack

The current situation in Japan totally depends on overseas industry to cryptanalyze (analyze) the virus

- At the contingency, there is a big challenge at chain of command. In Japan, there is NISC (National Information Security Center) which is a playmaker of security in Japan.

However, the 'lineup' is poor.

- There is a sectionalism among ministries and they are reluctant to corporate each other, not sharing information enough.

- Japanese people themselves need to get well-prepared. Most of the people do not pay attention on a daily basis.

In Japan National Information Security Center (NISC) was established within Chief Cabinet Office as a control tower on information security in April 2005 to coordinate horizontal and cross cutting enhancement as well as advanced information telecommunication network conference is located to advance the standard of information security of government and crucial infrastructure business operators and to enhance capacity more to deal with cyber attacks. NISC was set up reflecting the ministry targeted attack by anonymous in 2005.

Prime Minister Mr. Abe made a policy speech to the 183rd session of the Diet this February referring to reinforcing countermeasures and enforcing targeting cybercrimes and cyberattacks, which are menace to the Internet society.

This has led to the new efforts of The National Police Agency (NPA), which announced on March 2013 that Japan is set to launch a 140-strong nationwide police task force that would focus on fighting cyber crime, including attacks that come from overseas. The so-called cyber police are to be deployed in Osaka, Tokyo, as well as other strategic areas. The members are composed of specialists that have been recruited from private firms and are fluent in the English, Chinese, Korean and Russian languages and its primary goal is to go a level higher in protecting government organizations, defense contractors and private organizations that operate infrastructure in the country.

Also Ministry of Internal Affairs and Communications (MIC) launched Cyber Security Research Center (CYREC) this April 2013 aiming at developing defense technology utilizing practical detection to deal with cyber attack. The targets are to

establish the hubs for cyber security R&D institutes crystallizing of the wisdom of All Japan, to build practical as well as fundamental technology against new cyber attack, implement social experiment in terms of R&D, and enhance international collaboration with Europe, the United States and with Asian regions for cyber security. This approach is fine and good to widen network observing, strengthen information analysis and capacity for judgment, however, it does not make sense unless they are shared to make it to stronger measures.

In response to this, draft of The Cyber Security Strategy was s released May 2013 and is now open for public comment. Here is the gist of it the following. Information security environment change of is dramatically rapid. This should be a Japanese grand design to achieve mutual coordination among ministries. In the past three years, risk for this hyper-connected situation has been enormous, spreading and reached at a global level. The scale and scope has been expanding.

Cyber space has become crucial brain and synopsis for the activities of daily basis, social and economic, and administrative ones. Fusion and integration has accelerated.

Cyber space is imperative for Japan and it will be more expanded and penetrated further, seeking for addressing social challenges and for higher potential for economic growth and innovation, it has been paid attention to by world as driving force Now cyber attack against infrastructure turns into a reality and is a serious matter of national security and risk management Japan is aiming at the most advanced IT state in the world and needs to achieve safe cyber space to be suitable. The scope of the target of cyber attack is growing phenomenon from private (individual and family) to public (social infrastructure). The risk of cyber attack has been growing although Japan has made efforts to deal with it. The risk is getting worse and it has affected our national security and risk management as well as international competition, it brings enormous constant anxiety to Japanese people.

The basic aim of Cyber Security Strategy forging Cyber Security Nation is the following. Fundamental idea consists of four agendas; securing free information distribution, new efforts towards escalating risk, strengthening risk-based response, action and mutual assistance based on societal responsibility. Role of each player is clarified; nation, infrastructural enterprise, business industries (R&D institutes), users and cyber space involved operators.

Targeted focused areas until 2015 contains three bullet points ; government establishes a resilient cyber space improving the expansion of information security, strengthening against cyber attack, builds a vibrant cyber space activating

industries, accelerating R&D development further, fostering of human resources for information security utilizing competition, improve the information literacy of all the public, takes the lead in formulating cyberspace focusing on diplomacy, internationally expanding, international collaboration.

With regard to the driving force for cyber security in Japan, National Information Security Center (NISC) will strengthen the operation of cyber space. It will prepare a system for securing experts and authorities reorganizing as 'Cyber Security Center' with an opening date 2015.

Here are some functional norms to deal with Japan case.

- Global Common

- Fundamental Reforms for security architecture

- Citizen awareness

- Integrated strategy

Global commons (Recognition for the oneness of humanity)

• maintain consistency with existed international laws (regime for governance)

• Avoiding loss of strategic trust

• no scramble but peaceful use

• launch international platform

• peaceful and stable international order

• global responsibility (as a global citizen)

• Critical Thinking

• Ethical Discussions

• Accountability endorses the duty to transform information and knowledge for people another thought for functional norms.

Hedging strategy beyond engagement

• indirect hedging : dispersion of risk

• soft hedging: include unspoken country and launch consortium and build multi layers cooperation

• hard hedging: strengthen military capacity and build robust relationship with overseas (this is more traditional approach)

Challenge Cases

• Global minded education (awareness for citizen)

• Global user: this hyper-connected world will lead to more fragmented / fragile society

• facing black swan events (seeking for solution)

Here I believe that the definition of the global is necessary.

For Further Implication

We have to be careful about the term of 'global'. What is the international standard? Look at the map what you have. You would be surprised at what other countries have used and how different it is. The looks are not the same if you take a look at your country by globes. We should see where we are in a different perspective, well-poised to deal with cyber attack. Also, the viewpoint of citizens is brought into eyeing developing policies from such as public comment. Southeastern shift: The new leaders of global economic growth FT. To address cyber attack, we need to fine tune to have global white paper for cyber security?

Although people realize that defense might become a magnet for attack and mistrust makes itself more vulnerable to attack, they cannot help it since they also believe that pragmatic attitude is crucial for cyber issue as well.

Now ethics and philosophy element should be revisited to address the security and to analyze the new phase. These elements will lead to personality. The element of convergence imperative to discuss as a new phase as well.

As Gorguin says, where do we come from, what are we?, where are we going? Thomas Jefferson says that those who would give up Essential Liberty to purchase a little Temporary Safety, deserve neither Liberty nor Safety.

For Japan, cyber issue is a theme associated with the role as a sovereign nation, as 'self-help' nation. How Japan defined her responsibility in terms of US-Japan alliance, which is a basic guideline of national security of Japan? Should Japan redefine it? If so, how? How Japan should deal with new challenges caused by information evolution?

Acknowledgements

• Francis Bacon

• Alvin Toffler

• Japan Cyber strategy report May 2013

• FireEye Advanced Threats Report 1H 2012

• National Cyber Security Strategies- Practical Guide on Development and Execution December 2012

• Financial Times article ‘ nations are chasing the illusion of sovereignty’ 6 June 2013

http://www.ft.com/intl/cms/s/0/d1dcdb6a-cddb-11e2-a13e-00144feab7de.html#axzz2WqqIiyJz

• Science News (online) Mar 28, 2013 Japan police to launch national cyber crime force

• The Tallinn Manual on the International Law applicable to Cyber Warfare

http://www.ejiltalk.org/the-tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/

• Atlantic Council http://www.acus.org/new_atlanticist/reason-finally-gets-voice-tallinn-manual-cyber-war-and-international-law

DISCLAIMER: **The analysis contained in this paper is personal to the author and does not reflect the views of the JST/RISTEX.**

Кир Гилс
(Keir Giles)
Директор Центра исследований конфликтов
(Великобритания)

ВЗГЛЯД ЧЕРЕЗ КРИВОЕ ЗЕРКАЛО: РОССИЙСКИЕ ИНТЕРЕСЫ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРЕДСТАВЛЕНИИ ЗАРУБЕЖНЫХ ГОСУДАРСТВ

Предложенные Россией инициативы по стимулированию международного сотрудничества в области информационной безопасности были встречены остальными странами достаточно неоднозначно. В частности, какое-то время многие страны, в числе которых США и Великобритания, попросту их игнорировали. Подобная реакция как нельзя лучше свидетельствует о сохранившейся гигантской разнице в мировоззрении и предпосылках, которые вынесены в составе российских инициатив, и общем мнении евро-атлантического альянса в отношении принципов работы Интернета и его предназначения. В основе сложившейся ситуации лежит два кардинально противоположных понимания информационной безопасности. В настоящей работе сделана попытка разъяснить содержание российского предложения и идей для западной аудитории, чтобы сделать более понятным особенности их восприятия целевой аудиторией.

Проблемы и разногласия, представленные ниже, традиционно знакомы тем, кто напрямую участвует в международном обсуждении проблем информационной безопасности. В данной работе не делается попытка подробно описать все из них, поскольку детальное обсуждение приводится в исчерпывающем объеме в других трудах.[253] При этом не следует забывать, что дан-

[253] В качестве примера можно привести документ «Russia's 'Draft Convention on International Information Security' – A Commentary», Conflict Studies Research Centre, апрель 2012. Доступна на сайте http://conflictstudies.org.uk/files/20120426_CSRC_IISI_Commentary.pdf

ная международная группа в составе представителей обеих точек зрения, представляет собой весьма незначительную часть куда более обширного сообщества, задействованного в обсуждении вопроса в целом. Очень многие официальные лица, дипломаты, политики и консультанты из стран Запада знакомы с позицией лишь одной стороны спора, поэтому ниже обсуждаются лишь поднятые Россией вопросы и варианты решения их. Реакция на российские аргументы, действия и политические инициативы со стороны этой группы могут включать в себя такие выражения, как «непредсказуемо», «без должного проявления сотрудничества», «невразумительно» и даже «иррационально», и именно их мы постараемся разъяснить.

После первого ознакомления с российской позицией в вопросах информационной безопасности в Интернете специалисты, которые прежде не имели опыта общения с Россией, чаще всего демонстрируют последовательность из трех реакций: пренебрежение, затем непонимание, после чего следует инстинктивное или обоснованное отрицание. Мы последовательно изучим каждый из перечисленных этапов.

Пренебрежение

Международные дебаты по вопросу информационной безопасности долгое время характеризовались взаимным непониманием. Исключая тех, кто напрямую работал с Россией или Китаем, многие члены евро-атлантической коалиции в составе политических деятелей или представителей научных кругов попросту оставались в неведении относительно имеющейся совершенно иной точки зрения, которая кардинально отличается от привычной им позиции.

Отчасти это связано с потрясающим единодушием по обсуждаемой проблеме, в особенности среди англоговорящих наций, где сложно выделить хоть какие-то расхождения в подходах или основополагающих допущениях касательно роли и характера кибербезопасности. Подобный устоявшийся консенсус приводит к тому, что даже эксперты с немалым международным опытом не способны оценить тот факт, что в природе может существовать и иное мнение. Скажем, участники состоявшейся в Лондоне в марте 2013 года церемонии по принятию «Таллиннского руководства по международному праву, применяемому к кибербезопасности» встречались с таким описанием его всеобщего признания: «США, Великобритания, ЕС и НАТО единодушны. В целом, все согласны» - при этом не учитывается тот факт, что «все» охватывает куда больше стран, зачастую пропагандирующих совершенно иные подходы к обсуждаемому предмету.

Подобная ситуация отчасти возникает по причине относительно слабой информированности о ключевых предложениях России. Зачастую не делается даже попытки довести российские идеи до сведения более широкой публики. Можем в качестве примера привести состоявшуюся в октябре 2012 года в Будапеште конференцию по вопросам кибербезопасности, где впервые был сделан шаг на пути к объяснению остальному миру точки зрения России. Перед началом конференции на сайте для ознакомления были выложены «международные документы по кибербезопасности», где перечислялись национальные и международные подходы к кибербезопасности – например, текст речи шведского министра иностранных дел Карла Билдта, официальные документы Канады и Австралии касательно стратегии кибербезопасности, Будапештская конвенция о борьбе с киберпреступностью, рекомендации ОЭСР, заявления НАТО. Российские переводы представлены не были.[254] И в ходе самой конференции, как и в случае с проходившей годом ранее в Лондоне конференций о ситуации в киберпространстве, выступление на русском языке проходило без переводчика, из-за чего никто не смог понять ключевых моментов, отличающих позицию России от консенсуса в евро-атлантической зоне касательно Интернета, прав и обязанностей пользователей в киберпространстве. Частично это стало причиной того, что многие наблюдатели были неприятно удивлены осознанием факта нестыковки означенного консенсуса с мнением остального мира, что получило свое подтверждение на Всемирной конференции по международной электросвязи (WCIT) в Дубае в декабре 2012 года.

Непонимание

Даже после того, как становится очевидным наличие иной официальной позиции России в вопросах кибербезопасности, ее понимание оставляет желать лучшего. По большей части это вызвано тем, что многие предложения для международного одобрения, а также допущения касательно характера отношений в Интернете, положенные в основу предложения и продвигаемые российскими полномочными органами, напрямую конфликтуют с восприятием работы Интернета со стороны евро-атлантического сообщества. Скажем, ключевой составляющей российского предложения является идея национального информационного пространства под государственным управлением, однако это не соотносится с работой российских Интернет-провайдеров и органов, отвечающих за регистрацию доменов, которые не имеют привязки к государственным

[254] См. http://www.cyberbudapest2012.hu/national-cyber-documents - последний сеанс доступа 28 июня 2013 года

структурам и ежедневно обеспечивают свободу потоков информации меж границ, ведь именно в этом и заключается фундаментальная особенность Интернета. Как было отмечено на веб-странице Российского форума по управлению Интернетом, который состоялся в конце апреля 2013 года:

> Интернет является надгосударственным образованием и, де- факто, не имеет границ. Именно поэтому для Интернета так подходит модель коллективного управления Сетью (т.н. мультистейкхолдеризм).[255]

Это напрямую противоречит ряду ключевых принципов в составе российских инициатив на политическом уровне.

Указанная нестыковка в восприятии фундаментальных основ кибербезопасности охватывает и другие сегменты, где базовые принципы, выдвинутые правительствами других (кроме России) стран, не дают возможности полноценно понять некоторые из российских идей. В качестве иллюстрации можно уйти от хорошо известных заявлений США о сути кибербезопасности и взять, вместо этого, позицию Швеции, которую мы и изучим. По словам представителей министерства иностранных дел Швеции, а именно департамента международного права и защиты прав человека:

> Мы рассматриваем свободу в Интернете в рамках механизмов защиты прав человека... В основе лежит базовый закон о правах человека: безопасность должна быть организована таким образом, чтобы не нарушать... Информационная безопасность должна встать на защиту граждан, а не государства. Речь не идет о том, чтобы защитить меня или вас.[256]

Озвученное представление о том, что права человека являются фундаментальной истиной, определяющей принципы управления Интернетом, резко контрастирует с российским подходом, озвученным в публичных заявлениях, согласно которым первоочередное значение имеет безопасность, а прочие факторы вторичны. Швеция не единственная страна, высказавшая свое несогласие – позиция Великобритании такова, что в основе всего лежат экономические аспекты, и именно вокруг них надлежит выстраивать безопасность:

---

[255] Авторский перевод. См. сайт http://rigf.ru/about/, последний сеанс доступа 19 июня 2013 г.

[256] Йохан Халленберг, заместитель директора департамента международного права и защиты прав человека, Министерство иностранных дел Швеции, из выступления на Совете Европы по вопросу внешних отношений, 17 апреля 2013 года, Лондон

> Киберпространство в первую очередь связано с экономикой и процветанием. Национальную безопасность и военные интересы в данном случае можно отодвинуть на второй план.[257]

В целом допущение о том, что кибербезопасность призвана «защищать отдельных граждан, а не правительство», является общей темой, однако ни в коем случае не сопоставимо с российской формулировкой безопасности как средства защиты триединства гражданина, общества и государства.[258]

Дополнительные сложности связаны с тем, что российские политические заявления по этому и другим вопросам в значительной степени разнятся, в зависимости от источника, что вызывает еще большее непонимание за рубежом. Многие представители Министерства иностранных дел, Министерства внутренних дел, Министерства связи, Федеральной службы безопасности, Совета безопасности и Администрации президента (в двух последних случаях позиция озвучивается посредством курируемых ими научных учреждений, а именно Института проблем информационной безопасности и Российского института стратегических исследований) выступают с заявлениями, которые, справедливо или ошибочно, воспринимаются как голос официальных российских властей, но при этом противоречат друг другу. По этой и ряду других причин коммерческие образования в России и те, кто следят за обсуждаемым вопросом за рубежом, с нетерпением ждут обещанного выпуска новой Стратегии кибербезопасности, которая, предположительно, поможет прояснить хотя бы часть из наиболее противоречивых аспектов.

Упор на свободу самовыражения в качестве одного из прав человека вызывает аллергическую реакцию у иностранных наблюдателей при рассмотрении официальных заявлений из России, где многими видится призыв к регулированию мнений в социальных медиа. Подобные заявления, несмотря на их кажущуюся рациональность в рамках определенного контекста, воспринимаются за рубежом в атмосфере, которая подразумевает тотальную неприкосновенность свободы слова, то есть совершенно не приемлет варианта с любыми ограничениями для социальных медиа как средства волеизъявления.

[257] Кевин Теббит, бывший директор штаба правительственной связи и постоянный заместитель министра обороны Великобритании, выступая на всемирном стратегическом форуме, Палата Лордов, 21 ноября 2012 года, Лондон.

[258] Следует отметить, что Россия не единственная страна, которая в меньшей степени акцентирует аспект прав человека при обеспечении кибербезопасности. Когда страны Европы на Будапештской конференции настояли на рассмотрении прав человека, китайская делегация спросила, на какой конференции она находится – посвященной кибербезопасности, или правам человека.

Подобная убежденность настолько глубока, что некоторые страны берут на себя обязательства по оказанию содействия в поддержании свободы слова в других странах, независимо от того, как это соотносится с национальным законодательством таких стран. Возвращаясь к примеру Швеции, из выделенного этой страной бюджета на развитие отношений с зарубежьем, 20% уходит на «наращивание потенциала / поддержку демократии», включая «предоставление инструментов для успешного обмена информацией» в репрессивном окружении и «предоставление программ шифрования для активистов», чтобы гарантировать сокрытие такого обмена информацией от национального правительства и правоохранительных органов. Несмотря на то, что речь, по сути, идет о вмешательстве в «информационное пространство» чужого государства, которое Россия стремится предотвратить, подобные действия не рассматриваются Швецией как враждебные. По словам Карла Фридриха Веттермарка из департамента международного права и защиты прав человека Министерства иностранных дел Швеции, «нет никакой связи между поддержкой демократии, включая представление средств шифрования и передачи информации, и работой с правительством, которому противостоят активисты».

Отчасти подобная ситуация возникает на фоне практически полного отсутствия восприятия угрозы со стороны социальных медиа членами евро-атлантического сообщества. К счастью, есть конкретный пример, который наглядно демонстрирует, отчего Россия и прочие страны озабочены неправомерным использованием социальных медиа или, как выразился в конце 2011 года генерал-майор Алексей Мошков из Министерства внутренних дел России, почему «социальные сети, со всеми их преимуществами, часто несут в себе угрозу для основ общества".[259] Возьмите хотя бы пример восстания и гражданской войны в Ливии, где социальные медиа и онлайновые средства связи, оставшиеся вне правительственного контроля, сыграли ключевую роль в смене режима. Согласно информации из исследования, опубликованного Военно-морским колледжем США:

> Успешное противодействие правительственному контролю систем связи привело к свободе действий в кибернетическом и наземном пространстве. Подобная свобода действий сделала возможной традиционную военную помощь со стороны США и НАТО, по результатам которой оппозиция смогла реализовать физические задачи

[259] Интервью Российской газете 8 декабря 2011 года.

[260] Джон Скотт-Рейлтон, «Революционные риски: кибертехнологии и угрозы в ливийском восстании 2011 года», Revolutionary Risks: Cyber Technology and Threats in the 2011 Libyan

> по свержению режима Каддафи и проведению последующих выборов нового правительства.[260]

Если переводить описанную ситуацию в контекст российской озабоченности вопросом безопасности, имеем полное соответствие с заявлением заместителя директора ФСБ Сергея Смирнова, сделанным в начале 2012 года: «Новые технологии используются западными разведывательными службами для создания и поддержания постоянного напряжения в обществе с серьезными намерениями, в том числе и по свержению режима».[261]

При рассмотрении российских предложений за рубежом возникает еще одна очевидная нестыковка между российскими инициативами по стимулированию международной активности в сфере кибербезопасности и собственной плохой репутацией России, как страны с процветающей киберпреступностью. В опубликованной в 2011 году книге говорится:

> Учитывая громадный потенциал.. всестороннего отслеживания событий в Интернете, можно предположить, что Россия создает непримиримую, агрессивную среду для киберпреступников. И это при том, что Российская Федерация является одним из крупнейших центров мировой киберпреступности. Реальные возможности полиции сильно ограничены, тогда как количество реально привлеченных к ответственности преступников едва достигает двузначного показателя.
>
> Причина, хотя ее никто не называет, всем понятна. Российские киберпреступники свободны в своих действиях… при условии, что целью их атак являются Западная Европа и Соединенные Штаты. [262]

Подобное утверждение не кажется противоречивым ввиду относительно слабой информационной поддержки последних российских усилий, направленных на борьбу с киберпреступностью, а также непримиримой позицией коммерческих субъектов, в отличие от правоохранительных органов, в деле борьбы с преступностью. С учетом сказанного за рубежом крепнет мнение об отсутствии каких-либо изменений (и это самое мягкое описание) в попустительском отношении к киберпреступности и другим формам антисоциального поведения в Сети, включая деятельность «патриотически

Rebellion", Центр обучения борьбе с нерегулярными военными формированиями и вооруженными группами в Военно-морском колледже США, Newport RI, 2013.

[261] Выступление на встрече Региональной антитеррористической группы Шанхайской организации сотрудничества, 27 марта 2012 года.

[262] Миша Гленни, «Серый рынок: киберворы, киберкопы и вы», Knopf, 2011 г.

настроенных хакеров», ведущих разрушительную и противоправную работу в таких зарубежных государствах, как Эстония и Грузия, что, видимо, совпадает с российскими государственными целями на текущий момент. Действительно, видимое нежелание России преследовать киберпреступников, выбравших для себя заокеанские цели, полагается серьезным и разумным объяснением одновременному нежеланию присоединиться к Будапештской Конвенции по киберпреступности.

Отрицание

Все вышеперечисленное создает неблагоприятную среду для положительного приятия российских идей о характере и целях кибербезопасности и способствует низкой интенсивности значимых обсуждений того, что же именно несут в себе указанные идеи. В итоге формируется их отрицание, на инстинктивном уровне или в рамках разумного толкования, как и показано выше. По словам шведских дипломатов, предложенный Россией и другими странами в составе ООН Проект конвенции о международной информационной безопасности и международных нормах поведения «является для нас просто неприемлемым».

На самом деле, как высказался еще один, пожелавший остаться неназванным, скандинавский дипломат, некоторые страны намеренно отказываются от использования термина (даже если эта фраза лучше всего подходит для описания обсуждаемой темы) «информационная безопасность» в своих официальных заявлениях в связи с негативными ассоциациями, поскольку ее давно напрямую ассоциируют с нормативными выкрутасами России и Китая и предпочитают переформулировать в более приемлемый термин «кибербезопасность». В то же время официальные представители других стран, которые крайне осторожны в выборе выражений и особенно в признании конкретных государств нарушителями кибербезопасности, могут время от времени обозначать Россию и Китай как «главными оппонентами», но не в кибернетических конфликтах, а в обсуждении прав человека.[263]

На государственном уровне имеется масса примеров абсолютного провала в достижении не просто диалога, а даже уровня взаимного понимания, без которого нельзя перейти собственно к диалогу. Разговор между глухими продолжается, и всякий раз каждая из сторон не способна определить, как именно отреагирует собеседник на те или иные фразы. Сюда стоит отнести и непонимание такого момента, что считающаяся на Западе нормальной и непротиворечивой политика может восприниматься как угроза не только в России, но

[263] Частная беседа с автором, апрель 2011 г.

и других частях света. Например, когда Джузеппе Абамонте из Генерального директората ЕС по сетям связи, контенту и технологиям (DG CONNECT) во всеуслышание заявляет, что ключевой составляющей стратегии ЕС в сфере кибербезопасности является «сотрудничество с третьими сторонами и гарантия передачи наших ценностей», многие из аудитории и не задумаются, что значительной части стран попросту не хотелось бы получить из Брюсселя посылку в виде чужих ценностей[264] - на самом деле, именно подобные попытки передачи ценностей рассматриваются как прямая угроза информационной безопасности российской Доктриной информационной безопасности.[265]

В то же время те, кто следит за заявлениями России в том же правовом поле, вынуждены не только продираться сквозь множественные и взаимно противоречащие источники предлагаемых политических инициатив, описанных выше, но и недоумевать по поводу ряда утверждений, глядя на которые понимаешь всю нереальность их серьезного прочтения, как например, обстоит дело с нижеследующим ответом на шаги по совершенствованию защиты интеллектуальной собственности в онлайн-среде:

> Неужели вскоре страны мира позволят США и ее приспешникам преследовать любого из нас? По всей видимости, так оно и будет. Нас ожидает тотальное рабство человечества, надзирателем в котором будут фашистские Соединенные Корпоративные Штаты Америки.[266]

Можно, конечно, сказать, что комментарии независимых медиа не стоит воспринимать как официальную позицию России, но с должным восприятием возникают определенные сложности, когда в названии таких средств массовой информации встречаются слова «Голос» и «Россия».

Результат такой разительной разобщенности между радикально противоположными подходами к одной проблеме можно сравнить с другими направлениями стратегического противостояния между Россией и евро-атлантическим сообществом, среди которых предложения России о новом Договоре о европейской безопасности или возражения России в отношении планов размещения ракетных оборонительных систем в Европе и ря-

---

[264] Выступление на Конференции по вопросам кибероборонs и безопасности сетей 26 января 2013 года, Лондон.

[265] Согласно Доктрине информационной безопасности Российской Федерации от 2000 года, «духовные, моральные и культурные ценности граждан» подлежат защите от внешнего влияния.

[266] «Помните тот MP3-трек? Полиция уже в пути», сайт Голоса России, 10 декабря 2012 г.

дом с ней. Во всех упомянутых случаях российская позиция основывается на соображениях и доводах, которые совершенно несопоставимы с реальностью в том ее виде, какой она понимается европейской и северо-американской аудиторией. Как следствие, во многих случаях самым простым и наиболее подходящим ответом становится не стремление ознакомиться с непонятной точкой зрения России, а игнорирование ее в надежде, что рано или поздно она от нее откажется.

Keir Giles
Director, Conflict Studies Research Centre, UK

HALL OF MIRRORS – FOREIGN PERCEPTION OF RUSSIAN INFORMATION SECURITY CONCERNS

Initiatives put forward by Russia for international cooperation in information security have received a mixed response from other states. In particular, over a period of years they have been consistently ignored or rejected by the U.S., the UK and other like-minded nations. This response is indicative of a huge remaining divide between the views and assumptions expressed in the Russian initiatives and a very different Euro-Atlantic consensus on how the internet works and what it is for. Underlying this is a gap in comprehension between two very different approaches to information security. This paper seeks to draw on experience of explaining the Russian proposals and ideas to Western audiences, in order to outline how they are perceived by their intended audience.

The issues and contradictions described here will be wearily familiar to those directly involved in international discussion of information security; it is outside the scope of this short paper to describe them in detail, and they have been exhaustively listed elsewhere.[267] But it has to be remembered that this international group with exposure to both sides of the argument is only a very small subset of the much larger range of individuals engaged with the issues as a whole. Many more officials, diplomats, policy-makers and advisers in Western nations will only be acquainted with their own side of the debate, and it is their view of Russian concerns and proposed solutions that will be discussed here. The reaction to Russian statements, actions, and policy initiatives from this group can include words like "unpredictable", "unnecessarily uncooperative", "incomprehensible" and frequently "irrational", and it is this failure of communication which we will seek to describe.

First exposure to the Russian view of information security on the internet for those with no previous Russia expertise gives rise, as a rule, to a sequence of three reactions: ignorance, followed by incomprehension, followed by either instinctive or reasoned rejection. We will examine each of these phases in turn.

Ignorance

The international information security debate has long been characterised by mutual blind spots. Unless directly engaged with Russia or China, many in Euro-

[267] As for instance in "Russia's 'Draft Convention on International Information Security' – A Commentary", Conflict Studies Research Centre, April 2012. Available from http://conflictstudies.org.uk/files/20120426_CSRC_IISI_Commentary.pdf

Atlantic policy or academic communities remain simply unaware that there is a view which diverges sharply from the one they are accustomed to.

In part, this is because of the striking unanimity of view on the subject, particularly among English-speaking nations, where it is hard to identify any divergence in approach and underlying assumptions on the role and nature of cyber security. This deep consensus can give rise to a situation where even those experts with international exposure can overlook the fact that this is not the only possible view. For example, attendees at the London launch of the "Tallinn Manual on the International Law Applicable to Cyber Warfare" in March 2013 heard the following description of its universal acceptance: "The US, the UK, the EU and NATO all agree. Everybody agrees" - rather overlooking that "everybody" includes substantially more nations with a very different approach to the subject.

This situation derives in part from the relative lack of visibility of key Russian proposals. Opportunities to bring the Russian ideas to broader notice appear often not to be taken. We can take as an example the Budapest Conference on Cyberspace in October 2012, on the face of it a prime venue for explaining the Russian point of view to the world. Ahead of the conference, "International Cyber Documents" were provided for reference on its website, outlining national and international approaches to cyber security - for example, the text of a speech by Swedish Foreign Minister Carl Bildt, Australian and Canadian White Papers and Cyber Security Strategies, the Budapest Convention on Cybercrime, OECD recommendations, and NATO statements. Yet no Russian equivalent was provided.[268] And during the conference itself, just as at the London Conference on Cyberspace the previous year, a presentation delivered in Russian failed to account for interpretation and therefore failed to put across key points at which the Russian view diverged from the Euro-Atlantic consensus on nature of internet and rights and obligations in cyberspace. It was for this reason, among others, that many observers experienced considerable surprise when this consensus came face to face with the rest of the world at the World Conference on International Telecommunications (WCIT) in Dubai in December 2012.

Incomprehension

Even when it becomes clear that a distinct official Russian point of view on cyber security exists, it is often imperfectly understood. This is due in large part to the fact that many of the proposals for international agreement, and the assumptions about the nature of the internet which underlie them, are in direct conflict with how

[268] See http://www.cyberbudapest2012.hu/national-cyber-documents - last accessed 28 June 2013

the Euro-Atlantic community understands the internet to work - and, indeed, with the understanding of Russian internet authorities themselves at a working level. For instance, a key principle of the Russian proposals is the concept of national information space under state control - but this is not compatible with the work of Russian internet service providers and domain authorities, unrelated to the state, who on a daily basis ensure the free circulation of information across borders because this is a fundamental feature of the internet. As stated on the website of the Russian Internet Governance Forum, which took place in late April 2013:

> Интернет является надгосударственным образованием и, де- факто, не имеет границ. Именно поэтому для интернета так подходит модель коллективного управления Сетью (т.н. мультистейкхолдеризм)
>
> (The internet is a supra-governmental entity, and de facto has no borders. It is for this reason that the model of collective governance (so-called multistakeholderism) is so suitable for the internet.) [269]

This is in direct contradiction to some key principles of Russian initiatives at a political level.

The mismatch of fundamental notions of what cybersecurity is about extends into other areas, where basic principles espoused by governments other than Russia make it hard to understand some Russian ideas. For the purpose of illustration, we can avoid well-known US statements on cyber security, and instead take Sweden as a case study. According to Swedish Ministry of Foreign Affairs officials from the International Law and Human Rights Department:

> We analyse internet freedom within a human rights framework... The foundation is basic human rights law: security needs to be arranged so as not to violate human rights law... Information security is to protect the individual, not governments. It's to protect you and me.[270]

This notion that human rights are a fundamental concern determining how the internet should be managed contrasts with the Russian approach voiced in public statements that security is an essential basis and other considerations are secondary. Sweden is not the only country that disagrees: the UK view is that economic issues are the foundation and security has to be built around these:

---

[269] Author's translation into English. See RIGF website at http://rigf.ru/about/ last accessed 19 June 2013

[270] Johan Hallenberg, Deputy Director, International Law and Human Rights Department, Swedish MFA, speaking at European Council on Foreign Relations, London 17 April 2013

> Cyber is first about the economy and prosperity. National security and military security are not the most immediate concerns there.[271]

The overall assumption that cyber security is "to protect the individual, not governments" overlaps with but does not equate to the Russian formulation of security being about protection of the trinity of individual, society and state.[272]

An additional complication is that Russian policy statements on this and other issues differ widely depending on their source, giving rise to yet more incomprehension abroad. Officials from bodies including the Ministry of Foreign Affairs, the Ministry of Internal Affairs, the Ministry of Communications, the Federal Security Service, the Security Council and the Presidential Administration (the latter two, voiced through their academic offshoots, the Institute of Information Security Issues and the Russian Institute for Strategic Studies respectively) make pronouncements which rightly or wrongly are seen as voicing official Russian government policy, and which are mutually contradictory. For this reason and others, commercial entities in Russia and those following the topic overseas eagerly await the promised release of a new Cyber Security Strategy, which it is hoped will clarify at least some of the more controversial issues.

Emphasis on freedom of expression as a human right causes an allergic reaction among foreign observers when exposed to official Russian statements which appear to call for regulation of expression on social media. These statements, while they may appear entirely rational within context, are received overseas in an environment in which freedom of expression is sacrosanct, and which finds it inconceivable that social media, as a means of that expression, can be subject to restriction.

This conviction is so deep that some nations take upon themselves a mission to assist this free expression in other countries, regardless of whether this is in accordance with those countries' national law. Returning to the case of Sweden, of the Swedish overseas development budget, 20% is spent on "capacity building / democracy support" - including "providing tools needed to communicate successfully" in repressive environments and "providing encryption software for activists" to ensure this communication remains concealed from the national government and law enforcement authorities. Regardless that this constitutes the

[271] Kevin Tebbitt, former Director of GCHQ and Permanent Under Secretary of State for the UK Ministry of Defence, speaking at Global Strategy Forum, House of Lords, London 21 November 2012.

[272] It should be noted that Russia is not the only nation to place less emphasis on the human rights aspect of cybersecurity. Insistence by European nations on highlighting rights at the Budapest Conference led to a Chinese question of whether the delegation was at a conference on cybersecurity or on human rights.

kind of interference in another state's "information space" which Russia wishes to proscribe, this is not construed by Sweden as a hostile act. According to Carl Fredrik Wettermark, of the International Law and Human Rights Department, Swedish MFA, "there is no tension between democracy support - including encryption and communications provision - and working with the governments that the activists are opposing".

This arises in part because of an almost total lack of threat perception arising from social media among the Euro-Atlantic community. Fortunately, a case study is available to demonstrate why Russia and other nations are concerned over misuse of social media - or why, as expressed by Maj-Gen Aleksey Moshkov of the Russian Ministry of Internal Affairs in late 2011, "social networks, along with advantages, often bring a potential threat to the foundations of society".[273] This is the case of the uprising and civil war in Libya, where social media and online communication circumventing government control played a key role in regime change. According to a study published by the US Naval War College:

> Successful dispute of the government control of communications led to freedom of action in the cyber and land domains. This freedom of action led to traditional military support from the U.S. and NATO that ultimately allowed the opposition to achieve the physical objectives of defeating the Gaddafi regime and the eventual election of a new government.[274]

Translated to the context of Russian security concerns, this maps to statements like the one by FSB First Deputy Director Sergei Smirnov in early 2012: "New technologies are used by Western secret services to create and maintain a level of continual tension in society with serious intentions extending even to regime change."[275]

When Russian proposals are reviewed overseas, a further perceived incompatibility arises: between Russian initiatives for international action on cyber security and Russia's own bad reputation as a permissive environment for cyber crime. In a book published in 2011 it was stated that:

---

[273] Interviewed in Rossiskaya Gazeta, 8 December 2011.

[274] John Scott-Railton, "Revolutionary Risks: Cyber Technology and Threats in the 2011 Libyan Rebellion", United States Naval War College Center on Irregular Warfare and Armed Groups, Newport RI, 2013.

[275] Speaking at meeting of Shanghai Cooperation Organisation (SCO) Regional Anti-Terrorist Structure, 27 March 2012.

> Given the strength of... comprehensive surveillance of the Internet, one might assume that Russia would represent an implacably hostile environment for cyber criminals. Yet the Russian Federation has become one of the great centres of global cybercrime. The strike rate of the police is lamentable, while the number of those convicted barely reaches double figures.
>
> The reason, while unspoken, is largely understood. Russian cyber criminals are free... provided the target of [their] attacks are located in Western Europe and the United States. [276]

And this statement appeared entirely uncontroversial - because of a relative lack of publicity for recent Russian efforts against cyber crime, and the high profile of commercial entities, as opposed to law-enforcement agencies, in combating crime. The impression abroad persists, therefore, that there has been no change in the (at the very least) permissive attitude to cyber crime and to other forms of antisocial behaviour online, including the activities of "patriotic hackers" carrying out destructive and criminal activity in foreign states such as Estonia and Georgia, which happens to coincide with the Russian state aims of the day. Indeed, Russia's perceived unwillingness to prosecute cyber crime against overseas targets has been put forward as a serious and plausible explanation for the concurrent unwillingness to join the Budapest Convention on Cybercrime.

Rejection

All of the above creates an unforgiving environment for positive reception of Russia's ideas on the nature and purpose of cyber security, and contributes to the lack of meaningful debate on what precisely those ideas are. This leads to their rejection, either instinctive or reasoned as mentioned above. In the words of Swedish diplomats, Russia's proposed Draft Convention on International Information Security and the International Code of Conduct proposed by Russia and other states in the United Nations are simply "not acceptable to us".

In fact, as explained by another Nordic diplomat speaking anonymously, some states deliberately avoid any use of the term "information security" in official statements because of its negative associations; even if the phrase is the most appropriate one to describe the topic under discussion, it has been sufficiently tainted by association with the regulatory stance adopted by Russia and China in particular, that it is shunned in favour of the more acceptable "cyber security". Meanwhile, official representatives of other states which are deeply cautious about naming specific states as cyber security offenders overall can casually refer to Russia, China as the "worst adversaries" - not in cyber conflict, but in

[276] Misha Glenny, "DarkMarket: Cyberthieves, Cybercops and You", Knopf, 2011.

discussion over human rights.[277]

At a public level, examples abound of a total failure to achieve not just dialogue, but the level of mutual comprehension which would be its essential precursor. The dialogue of the deaf continues, with a failure on each side to appreciate how statements will be perceived by the other. This includes a lack of understanding that policy which is taken as normal and uncontroversial in the West can appear threatening not just in Russia but in other parts of the world as well. For instance, when Giuseppe Abbamonte of the European Commission's Directorate General for Communications Networks, Content and Technology (DG CONNECT) states publicly that a key part of EU cyber security strategy is «engaging with third parties and **making sure that we export our values**», many of those hearing him will not take into account that there are substantial parts of the world which do not wish to have their values exported to them from Brussels[278] - and in fact, precisely this kind of export is construed as a direct information security threat in Russia's Information Security Doctrine.[279]

Meanwhile, those following Russian statements in the same field have to contend not only with the multiple and conflicting sources of apparent policy initiatives as described above, but also with accompanying statements which can leave them disinclined to take what they read seriously - as, for instance, with the following response to moves for improved protection of intellectual property online:

> Is the world about to allow the US and its surrogates to come after all of us? Apparently it is. The total enslavement of mankind will soon be here, brought to you by the fascist United Corporate States of America.[280]

It can be argued that commentary in independent media should not be taken as representative of an official Russian position, but this is harder to argue when the name of the media outlet is in fact "Voice of Russia".

---

[277] Private conversations with author, April 2013.

[278] Speaking at Cyber Defence and Network Security conference, London, 26 January 2013 - emphasis added.

[279] According to the Information Security Doctrine of the Russian Federation, 2000, "spiritual, moral, and cultural values of citizens" should be protected from outside influence.

[280] "Remember that MP3? The police are en-route", Voice of Russia website, 10 December 2012.

The result of this disconnect between radically different approaches to the same issue can be compared to other areas of strategic contention between Russia and the Euro-Atlantic community, such as Russia's proposals for a new European Security Treaty, or Russian objections to plans for basing missile defence systems in and around Europe. In all of these cases, the Russian position is based on considerations and assumptions which are wholly incompatible with reality as it is understood by the European and North American audience. The result, in many cases, is that what often seems the simplest and most appropriate response to them is not to engage with the incomprehensible Russian view, but simply to ignore it and hope it will go away.

Филипп Бомард
(Philippe Baumard)
Профессор Политехнической школы
Президент Научного совета
французского Высшего совета
стратегических исследований

СРАВНЕНИЕ НАЦИОНАЛЬНЫХ ПОДХОДОВ И ДОКТРИН КИБЕРБЕЗОПАСНОСТИ

В статье исследуются технологические аспекты эволюции форм информационной преступности с момента ее появления в начале 1980-х годов до самых последних проявлений в 2013 г. Исследуя эту эволюцию, мы делаем выводы касательно доктрин, политических решений, инновационных стимулов и планов действий, предполагая возникновение новой парадигмы “поведенческого интеллекта”, с точки зрения как нападения, так и защиты.

Под киберпреступностью понимается противозаконное использование цифровых, электронных и программных средств, направленное на неправомерное применение общедоступных или частных информационных систем, вмешательство в их работу, лишение смысла получаемых ими результатов, влияние на них или их уничтожение. Нанесение ущерба компьютерным и информационным составляющим может и не являться основными целями или конечными результатами действий киберпреступников.

Возникновение киберпреступности сопутствовало деятельности пионеров в сфере новых технологий, с энтузиазмом исследовавших возможности, которые открывали технические инновации. Исследовательский интерес и независимое присвоение до сего момента остаются главными мотивационными стимулами при создании хакерских программ. Джон Дрейпер (John Draper) был одним из таких компьютерных энтузиастов, который помог популяризировать первую попытку “фрикинга”, состоящую в применении многочастотного звукового генератора, позднее получившего название “Blue Box”, подающего сигнал точно на частоте 2600 Гц для взлома телефонной системы дальней связи AT&T в начале 1970-х годов.

Большинство атак на ранних этапах были спонтанными, вызванными духом исследования новых технологий, ненаправленными (не предполагающими конкретных целей) и дающими немедленный эффект. С распространением персональных компьютеров эти хакеры-пионеры начали спонтанно образовывать объединения, разделяющие идеи гражданских свобод, сопротивления властям, и азарт обхода новых технологических решений. Практика фрикинга и хакерских атак стали факторами, надолго обусловившими дружбу разработчиков, пионеров отрасли (Возняк (Wozniak), Джобс (Jobs) и т.д.) и служившими политическими стимулами для действий энтузиастов от технологии. Границы между вновь возникающими культурами андерграунда (хиппи, хакеры) и криминальной субкультурой были расплывчаты и нестабильны, практики саморегулирования практически не существовало; в них входили подростки, "продвинутые" разработчики компьютерных программ и самостоятельно выучившиеся исследователи в новых технологических сферах. Этот период мы называем "эрой декодирования"; талантливые индивидуумы по большей части руководствуются соображениями чисто символической или весьма незначительной выгоды, чувства принадлежности к новым сообществам и самоидентификации.

Тем не менее, в середине 1980-х годов в системах электронных досок объявлений, посвященных техническим вопросам, которые поддерживали хакерские группы, начали публиковаться планы атак нападений, иногда одновременно физических и программных (см., например, первый выпуск Технического журнала группы Legion of Doom LOD/H от 1 января 1987 г.[281]). Впоследствии LOD и MOD (Masters of Deception) стали влиятельными группировками, преобразовавшими эти ранние группы в более организованные общины «взломщиков», сделавшими шаг в сторону от исходной культуры хакеров (см. Рис. 1).

[281] http://www.textfiles.com/magazines/LOD/lod-1

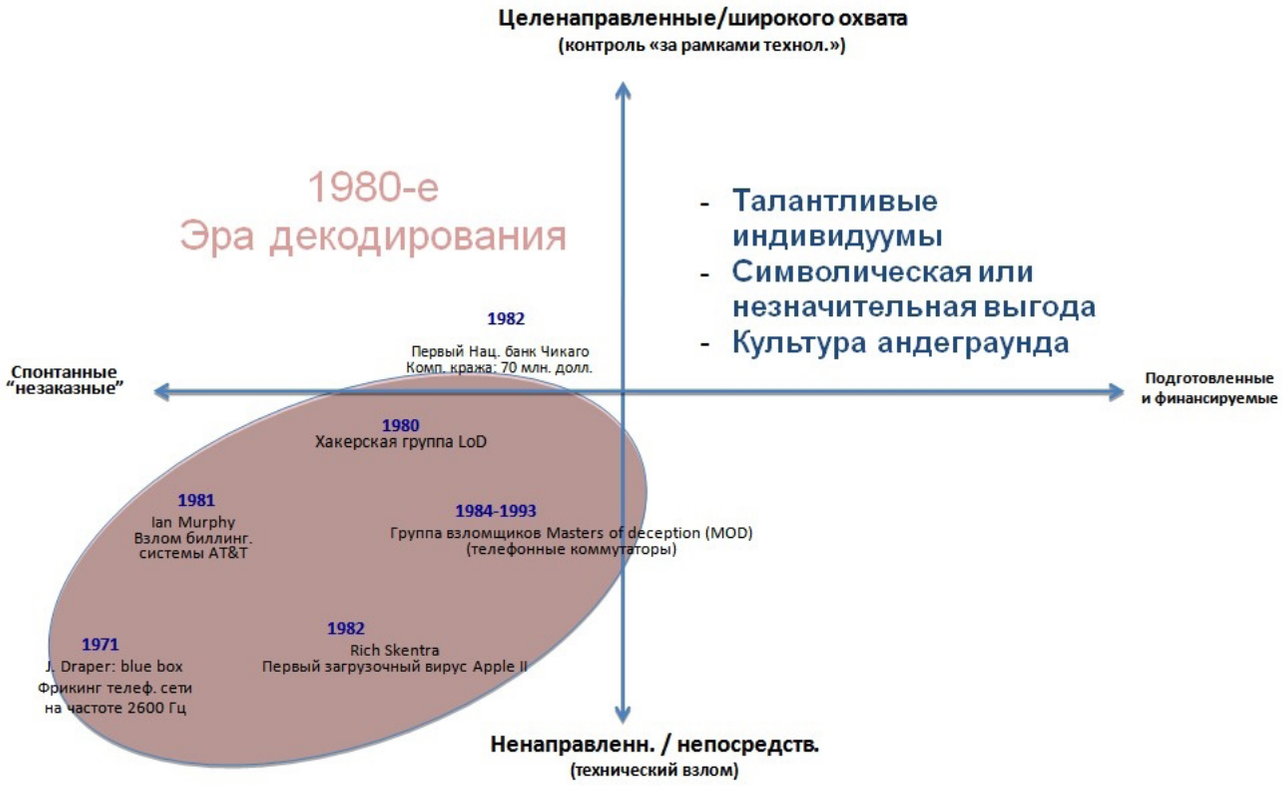


Рис. 1: Ранние годы: парадигма декодирования

Холодная волна и подпольная битва за освобождение Берлина сыграли определяющую роль в развитии хакерской культуры конца 1980-х годов. Происшествие с Клиффордом Столлом (астрономом из Национальной лаборатории имени Лоуренса в Беркли, случайно обнаружившим, что на компьютер в его лаборатории ведется вторжение из Западной Германии) было первым случаем, в котором был поставлен вопрос о важности координации работы разных агентств и сложности установления авторства международных компьютерных атак (Stoll, 1989). Этот пример был также одним из первых (1986) симптомов сформировавшихся в дальнейшем постоянных угроз высокого уровня, указавшим на сложность и изощренность кампаний вторжения (подробности смотри в статье Столла по адресу[282]). Соответственно, начало 1990-х годов сопровождалось возникновением субкультуры преступного хакерства. В 1980-х годах факты компьютерного взлома, приводившие к хищению или масштабным атакам, были редки. Двумя значительными исключениями были логическая бомба Pak Brain (1986), получившая известность как первый вирус, и компьютерное похищение 70 миллионов

[282] http://pdf.textfiles.com/academics/wilyhacker.pdf

[283] http://www.textfiles.com/hacking/modbook4.txt

долларов из Первого национального банка Чикаго (1982). «Великая война хакеров» (конфликт между группировками Masters of Deception и Legion of Doom, около 1991-1992 гг.) служит примером - сегодня, впрочем, нередко считающимся излишне преувеличенной личной конфронтацией - динамики межличностных отношений в начале 1990-х годов. Основным мотивом этих конфронтаций на раннем этапе была смесь желания повысить собственную значимость, показной храбрости и легкомысленности[283]. При этом, однако, публикация сведений о вторжениях хакерских групп, пробудило интерес правоохранителей. Последующая операция Sundevil в 1990 г. была первой масштабной операцией по обеспечению кибербезопасности в 15 городах США, в результате чего было произведено три ареста[284]. Большинство киберпреступлений были связаны с перехватом телефонных разговоров и подделкой телефонных и кредитных карточек. В результате оказавшейся не слишком успешной операции федеральные агентства стали серьезнее относиться к важности отражения кибератак (Sterling, 1994).

Публикации, подобные 2600, и возникновение киберпространства внесли свой вклад в демократизацию технологий взлома, фрикинга и хакерских атак, в результате чего они стали более разнообразными и пригодными для использования «вне технологических рамок». Сосредоточенность на дистанционном управлении и угрозы действия резидентных вирусов (распространенность троянов) повысили организованность криминальной субкультуры и привели к появлению общественной реакции на атаки: (см. Рис. 2).

[284] Clapes, Anthony Lawrence (1993). Softwars : the legal battles for control of the global software industry. Westport, Conn.: Quorum Books

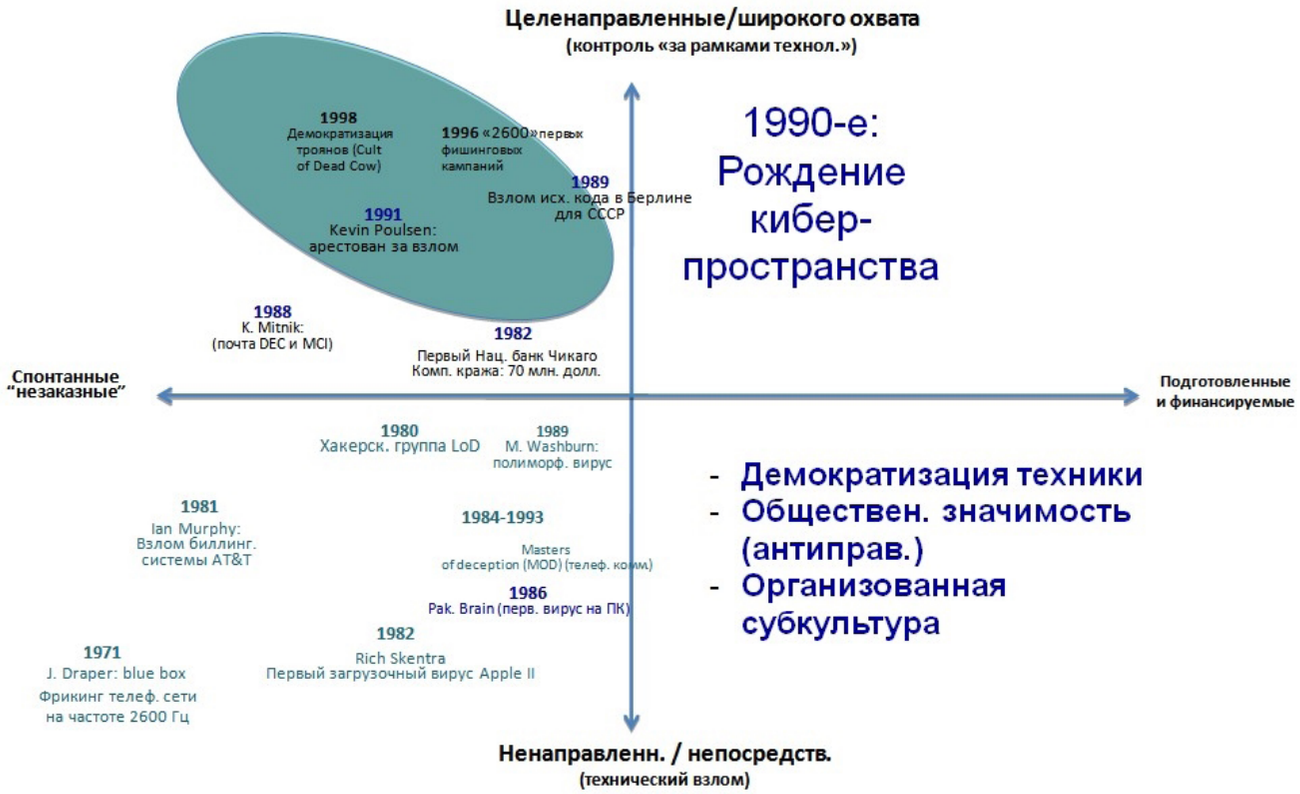


Рис. 2: 1990-е: демократизация киберпреступности

В то время как целью готовящейся атаки является единственная точка нападения, в начале 2000-х происходит обращение к абсолютно новому сценарию. Развитие электронной коммерции означает переход к коммерциализации киберпреступности, при котором организованная преступность приносит крупные доходы. Внедрение цифровых технологий в сферу культуры (MP3) повысило привлекательность взлома и повсеместное его распространение. Соответственно, профили деятельности хакеров изменяются в двух направлениях: с одной стороны, взломщики-любители (дилетанты и массовые потребители) начинают использовать имеющийся инструментарий, не имея глубокого опыта работы с ним (обмен файлами в формате P2P, рипование компакт-дисков); с другой стороны, производство вредоносных программ становится прибыльным черным рынком. Происходит быстрая монетизация услуг по имитации доменных имен, проведению атак на отказ в обслуживании, кампаний по нарушению работы сайтов и краже корпоративных данных. На 2000-2002 гг. приходится пик разработки вредоносных программ, в частности вирусов ILOVEYOU, Klez.h., Code Red и т.д. Группа Anonymous создана в 2003 году как сообщество слабо связанных между собой и спонтанно координирующих свои усилия лиц с раз-

личными интересами, от антиправительственных выступлений до обмена технологиями взлома и графическими материалами на платформе 4chan. На ранних этапах (2003-2006) массовые атаки и выступления, известные как «атаки 4chan», привели к популяризации представления о мотивах хакерской деятельности как смеси антиправительственных настроений, хулиганских побуждений и кампаний по осмеянию любых нежелательных явлений, хотя и с уклонением от участия в политических кампаниях.

В то же время, подготовка и спонсорская поддержка масштабных атак также наращивают обороты по мере ослабления ключевой философии хакерства, основанной на ценностях свободы личности и антиправительственной направленности, что связано с распространением встроенных хакерских инструментов и библиотек. Titan Rain (2003-2006) является примером первых попыток применения кибероружия с использованием методов простейших технологий в продвинутых кампаниях (см. Рис. 3).

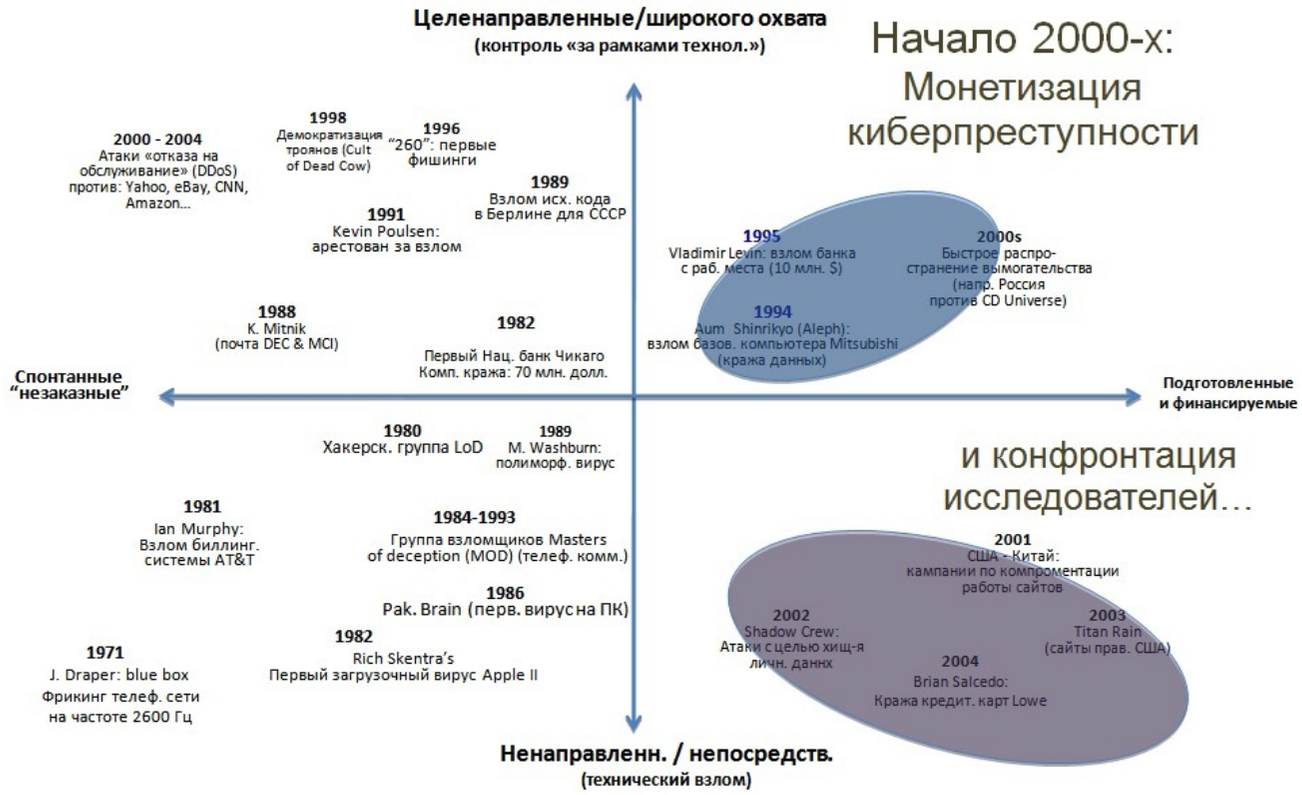


Рис. 3: Монетизация киберпреступности и первые государственные конфликты

Для 2005-2013 гг. характерны двойной сдвиг парадигмы и, в некоторой степени, совпадение целенаправленных и финансируемых кампаний, проводимых государствами или организованной преступностью, и более распространенных спонтанных и обширных кампаний, проводимых группами антиправительственных активистов, командами хакеров и слабо организованными сообществами наподобие Anonymous и LulzSec. Для этого периода также типичен быстрый рост стратегических и политически мотивированных атак (Kerem125, нацеленный против ООН, китайская кампания APT1 мирового масштаба, эстонские DoS атаки, Stuxnet, операция Aurora...) (Рис. 4).

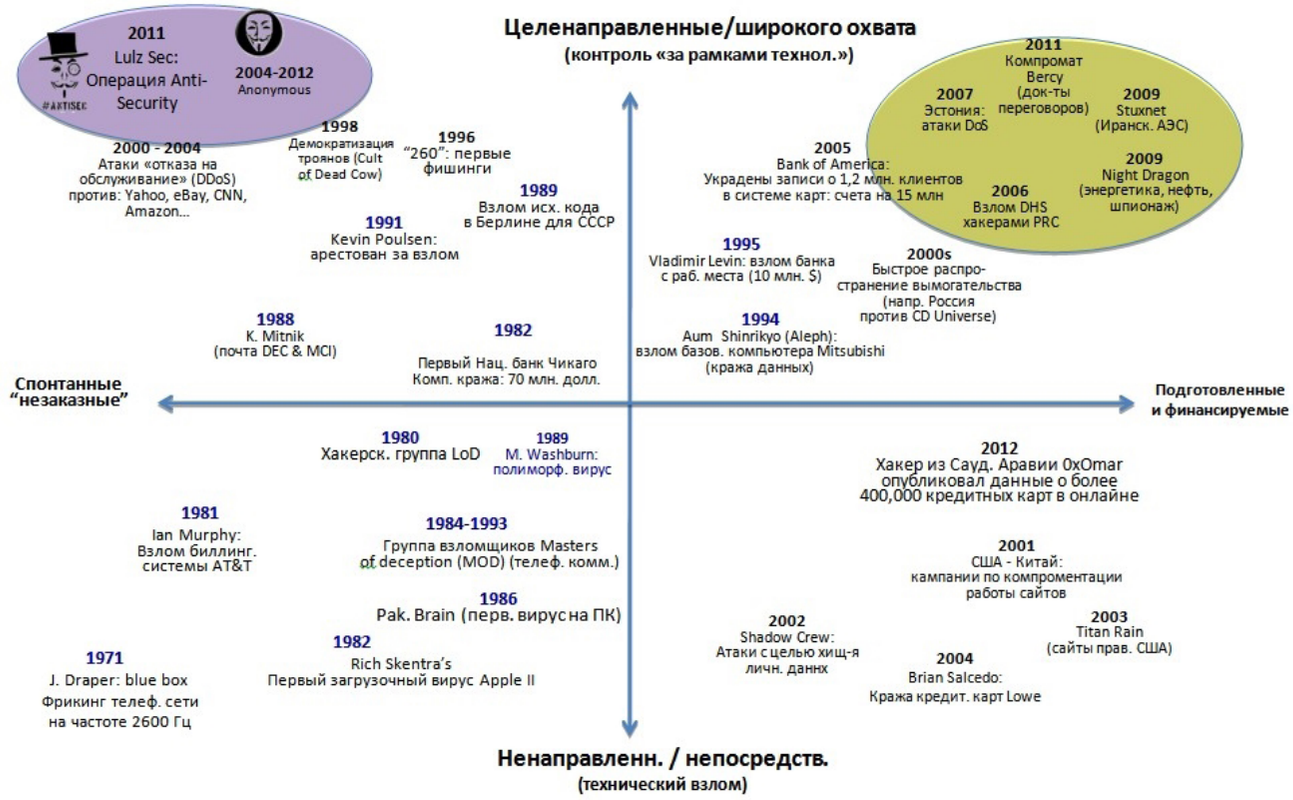


Рис. 4: За рамками технологии: начало крупномасштабных целевых кампаний (2005-2013)

Технология, используемая в этих масштабных кампаниях, не отличается от приемов на заре хакерства каким-либо радикальным образом. 125 строк кода столь же эффективны и в 2013 г., также способны использовать уязвимости систем, даже при том, что объем кода оборонного за последние 25 лет вырос в разы. Наиболее инновационной идеей в начале 21 века стала реализация этих кампаний на основе доступности и распространенности комбинаторного обучения, т.е. умения опережать развитие оборонного потенциала целей с применением средств сбора данных, превосходящих противника по качеству и быстродействию.

Формирование двух четко отличающихся моделей (масштабных спонтанно формирующихся групп и финансируемых целевых масштабных кампаний) является указанием на два пути, которые могут быть использованы при достижении превосходства в коллективном поведенческом обучении. Большие спонтанно формирующиеся группы получают выгоду от дистанционного умелого обучения, т.е. обучения, проводимого отдельными хакерами, способными координировать усилия в очень крупных масштабах, что делает процесс коллективного обучения вездесущим и эффективным. Выгода при реализации целенаправленных финансируемых кампаний (например, APT) состоит в развитии автоматических алгоритмов искусственного интеллекта (ИИ), встраиваемого в технологические решения (напр., Stuxnet, FLAME).

Большинство оборонных систем основаны на распознавании сигнатур («встроенного вредоносного кода») злонамеренных программ или нормативном анализе моделей поведения при сравнении их со «здоровыми образцами» (системы выявления с использованием баз данных). На данный момент коллективный потенциал обучения спонтанно формирующихся групп и потенциал машинного обучения на базе сигнатур опережают системы выявления на базе сигнатур. Природа данного сдвига парадигмы в этом смысле весьма схожа с эволюцией информационных средств ведения войны в начале 1990-х. Мы становимся свидетелями стратегического разрыва, в условиях которого защищающаяся сторона консолидирует свою информационную инфраструктуру, в то время как нападающие ведут информационную войну (Baumard, 1994). Благодаря тонкому анализу, большая осведомленность может быть результатом рассмотрения обрывочных и частичных данных. Более подробная информация, однако, редко способна победить даже плохо сформированную осведомленность.

Парадигма *поведенческого интеллекта* идет рука об руку с неизбежным усилением «угроз нулевого дня». Всепроникающее, легкодоступное комбинаторное обучение позволяет множество путей компьютерного вторжения

(то есть использования уязвимых мест систем) в течение первых 24 часов после их обнаружения. Повторные формирование и комбинирование вторжений с использованием необнаруженных ошибок («атаки нулевого дня») возможны благодаря развитию каузальных технологий обучения или, при невозможности использовать их, очень большому числу спонтанно формирующихся хакерских групп и обмену сведений об их экспериментах по комбинированию. В рамках этой парадигмы сосредоточенность на стратегии защиты «по факту», основанной на сведениях об известных и выявленных уязвимостях, по всей вероятности, приведет к поражению.

Подвергаем собственные доктрины проверке подвижками в технологиях

Собрав данные об опубликованных доктринах кибербезопасности из открытых источников, во второй части нашего анализа мы делаем попытку оценить правильность доводов этих кибердоктрин, выдвигаемых ими при отражении угроз, базирующихся на поведенческом мышлении. Нами проанализированы данные о 38 национальных стратегических документов о борьбе с киберпреступностью, реализации кибероборонs и повышении устойчивости информационных инфраструктур и усовершенствования кибербезопасности.

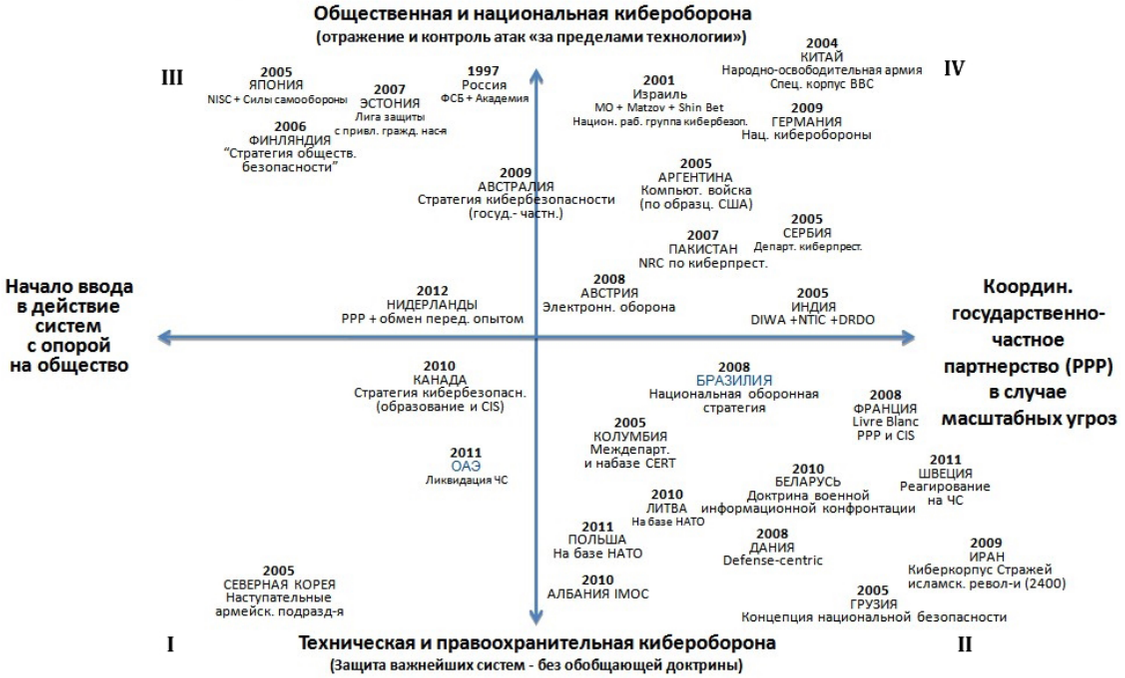
При разнесении видов киберпреступности по четырем категориям мы пользовались рамочной структурой, разработанной ранее при изучении истории вопроса, исходя из соображений конечного назначения действий («целенаправленные, с большим охватом» в отличие от “сиюминутных или ненаправленных») и их подготовленности («спонтанные», в отличие от «подготовленных и финансируемых»). Таким образом, мы выделяем четыре класса киберпреступников: «code warriors (воители)» (I), «cyber free riders (вольные стрелки)» (II), «autonomous collectives (независимые команды)» (III) и «sponsored attackers (финансируемые взломщики)» (IV).

Различные виды атак требуют различной реакции. Сиюминутные, спонтанные атаки (класс I) можно отражать путем налаживания прочной системы информационной безопасности, включая каузативное обучение, способное справляться с ухищренными атаками ИИ. В большинстве национальных доктрин правильно понимается реакция на такие атаки и предусматривается соответствующий спектр контрмер. Подготовленные и финансируемые прямые атаки (компьютерная кража в рамках организованной преступной деятельности, фишинг, взлом - класс II) требуют широкого спектра организованных технических и правовых контрмер. Системы сигнатурного выявления и оборонные меры с применением БД обычно являются достаточными контрмерами для отражения большей части угроз при наличии законодательной основы правоприменения. Социально или общественно обусловленные атаки (антиправительственные хакерские группы, кратковременные объединения управляемых общими целями групп на основе политических, социальных или экономических мотивов - класс III) предполагают ведение репутационных и информационных военных действий и наличие смыслоформирующего потенциала для реагирования на быстротечные и внезапные распределенные нападения. Наконец, наступательные действия с применением встроенного поведенческого интеллекта (класс IV) требуют перекрестного реагирования, охватывающего меры творческого реагирования «за рамками технологии» и

«за рамками притязаний». Угрозы класса III и IV требуют распознавания в реальном времени в беспрецедентных масштабах, подразумевающих масштабное когнитивное обучение человека с одной стороны (III) и масштабное поведенческое обучение с другой стороны (IV).

Наш анализ эволюции национальных доктрин киберпреступности за период с 1994 по 2013 год дал разнородные результаты. *Доктрины типа «Power-sovereign (Диктатор)»* (P-S, класс IV) делают ставку на крупные специализированные организации, нередко одержимы идеей защиты критически важных инфраструктур, и предполагают разработку, более или менее явную, наступательного потенциала. Хотя они и обеспечивают сбалансированную политику отражения финансируемых на уровне государства кибератак, обычно в их рамках развивается жесткая логика доминирования по отношению к угрозам, что вредит их вовлеченности в текущие перемены общественного характера. Соответственно, риск доктрин типа P-S состоит в отрыве от возникающих хакерских движений и недостаточной способности реагировать на распределенные когнитивные военные действия. *Доктрины типа «Societal Resilience (Общественное сопротивление)»* (класс III), с другой стороны, проявляют большую чувствительность к изменениям общественного мнения, пытаются воздействовать на общественное пространство и сосредотачивают свой наступательный потенциал на информационной войне. Мотивация этих доктрин далеко не всегда зиждется на демократических и прогрессивных взглядах на Интернет. При этом, однако, цифровое будущее общества явно определяется и как главная угроза, и как главная возможность развития кибероборонны и компьютерной сферы в целом. Наконец, доктрины «Social order (Общественный порядок)» (Класс I) и «Technocratic (Технократия)» (класс II) различаются только своим пониманием контроля. Основное различие кроется в том, что одна предполагает контроль на входе (I), а другая - исправление последствий (II). Технократические взгляды нередко страдают задержкой в понимании технологических изменений, вызванным философией реагирования на раздражители или запоздалым выходом в данное поле. Доктрины, отдающие предпочтение общественному порядку, обычно страдают недостатком государственного видения или государственного стратегического подхода или строят соответствующую тактику, заимствуя внешние идеи других государств или приводя свои идеи в соответствие с чужими.

На графике ниже представлено положение различных национальных стратегий противодействия киберпреступности и кибероборонны (год указывает дату публикации первого проанализированного документа). Результаты представляют собой компромисс между национальными тактическими решениями, сосредоточенными на киберпреступности, и решениями, основанными на контроле общественных корней прогресса в компьютерной сфере или их поддержке. Интересно отметить, что российская кибердоктрина ближе к возникающим «общественным» образцам, чем соответствующие положения Китая или США.



Оценка надежности национальных стратегий: чего ожидать?

Большая часть изученных национальных стратегий в отражении атак киберпреступников отстает от технологического прогресса лет на десять-пятнадцать. Соответственно, потрясения, затрагивающие общество в целом, систематически остаются вне поля зрения. Обычно подготовка киберполитики происходит в четвертом классе, в то время как наиболее разрушительные изменения происходят в третьем.

В период с 1990 по 2012 год основные хакерские технологии оставались на достаточно стабильном уровне. Стойкие угрозы продвинутого технологического характера (APT) сами по себе являются не результатом спада ключевых вторжений, но, скорее, изменением парадигмы, связанным с периферийными технологиями (в основном: машинным обучением, автоматизацией, комбинаторной конфигурацией). Такое изменение парадигмы процветает благодаря устареванию инфраструктуры. Комбинации возможны, когда ошибки могут использоваться кросс-системно. Все возрастающая способность уязвимых систем к взаимодействию увеличивает вероятность импровизированной эксплуатации кросс-системной уязвимости. В таком контексте разработчики, принуждая противодействие киберпреступности сводить к оценке уязвимости «точек доступа», мешают производить инвестиции в поведенческие технологии обучения (поддерживая малоэффективную, но чрезвычайно доходную сигнатурную парадигму обороны).

Единственным способом противостоять интеллектуальному поведению и реагировать на него является способность обогнать и перехитрить поведенческий интеллект. Лишь в очень немногих изученных доктринах признавалась эта ключевая системная уязвимость. Меры по укреплению доверия и безопасности (CBSM), соответственно, основываются на понимании технологических и общественных факторов, которые могут стать причиной уязвимости, и оказываются в значительной степени слепы к природе будущих технологических угроз.

Национальные доктрины технократии (класс II) и социального порядка зависят от вертикального развития и правового опыта, в то время как эволюция угроз идет горизонтально и противоправно. Последние крупномасштабные кампании (APT1, Blaster-worm, и т.д.) продемонстрировали ограниченность координации усилий различных правоохранительных органов при реагировании на атаки с непредсказуемым авторством, неизвестными или невыявленными сигнатурами и при использовании каузативного обучения для адаптации к часто встречающимся техническим средствам реагирования.

Большая часть проанализированных доктрин продемонстрировала устаревший подход к понятию авторства и атрибуции. В большинстве доктрин установление авторства соотносится с географической точкой ввода (или несколькими точками), основной целью атаки и формальными перспективами отслеживания источника атаки. Хакерское сообщество давно преуспело в деле уничтожения следов присутствия или вторжения, что позволяет сделать вывод, что дипломатические усилия направлены на разрешение вопроса, который потерял техническую значимость еще до 2007 г.

По мере нашего вхождения в очередной «пионерский» период, странным образом напоминающий годы расцвета фрикинга в хакерской деятельности (1972-1978), критически важным становится понимание социальной психологии развития угроз. Любопытно, что среди предположений, содержащихся в большинстве национальных стратегий, полностью отсутствуют повышение мобильности машинного обучения (загружаемого, распределенного или полностью автономного). Причиной этого может быть перенос принципов эскалации военного потенциала (гонка вооружений, сосредоточение, возможность принятия решений) на противодействие киберпреступникам. Кибернетические наступательные шаги не соответствуют традиционным моделям эскалации и подкрепления. Они черпают силы для повышения своего злонамеренного потенциала из своей способности трансформироваться, распределенного характера, и возможности обучаться быстро и независимо.

Литература

1. Barreno Marco, Peter L. Bartlett, Fuching Jack Chi, Anthony D. Joseph, Blaine Nelson, Benjamin I. P. Rubinstein, Udam Saini, and J. D. Tygar (2008), "Open Problems in the Security of Learning", *First ACM Workshop on Security and Artificial Intelligence (AISec),* pp. 19-26, Alexandria, Virginia.

2. Baumard, P. (1994), «From Information Warfare to Knowledge Warfare: », in : W. Schwartau (Ed.) (1994), *Information warfare*, New York : Thunder's Mouth Press, pp. 611-626

3. Bodmer, Kilger, Carpenter, & Jones (2012). Reverse Deception: Organized Cyber Threat Counter-Exploitation. New York: McGraw-Hill Osborne Media.

4. Gaycken, Sandro (2012) "Die sieben Plagen des Cyberwar," In R Schmidt-Radefeldt & C Meissler, C. (eds.), *Automatisierung und Digitalisierung des Krieges*, Berlin: Forum Innere Führung.

5. Rubinstein Benjamin I. P., Blaine Nelson, Ling Huang, Anthony D. Joseph, Shing-hon Lau, Satish Rao, Nina Taft, and J. D. Tygar, (2009), "ANTIDOTE: Understanding and Defending against Poisoning of Anomaly Detectors", IMC '09: *Proceedings of the 9th ACM SIGCOMM on Internet Measurement Conference*, pp. 1-14, Chicago, IL.

6. Sterling, Bruce (1994). "Part Three: Law and Order". The Hacker Crackdown: Law And Disorder On The Electronic Frontier. New York: Bantam Books.

7. Stoll, Cliff (1988), "Stalking the wily hacker", Communications of the ACM, 31(5), pp. 484-500.

8. Stoll, Cliff (1989), The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, New-York: DoubleBay.

Philippe Baumard
Ecole Polytechnique,
President of the Scientific Council of the French High Council
for Strategic Research

COMPARING NATIONAL APPROACHES AND DOCTRINES IN CYBER-SECURITY

This paper investigates the technological evolution of cyber-crimes form its emergence in the early 1980s to its latest developments in 2013. From this evolution, we draw implications for doctrines, policy, innovation incentives and roadmaps as we propose the emergence of a new "behavioral intelligence" paradigm, both in the attack and defense arenas.

Cyber-crime refers to the unlawful use of numeric, electronic and software capabilities to misuse, temper, devoid, destruct or influence public or private information systems. Cybernetic and informational components may not be the primary target or final outcomes of cyber-crime campaigns.

The origins of cyber-crime are concomitant with the pioneering efforts of technology enthusiasts in exploring the possibilities offered by technological innovation. Exploration and autonomous appropriation are stil, to date, a core motivation in the creation of "hacks". John Draper was one of these computer enthusiasts who helped popularize the first "phreaking" hack, consisting of a multi-frequency tone generator, late known as the Blue Box to pitch the exact 2600 Hz frequency to hack into the long distance phone system of AT&T in the early 1970s.

Most of early attacks were spontaneous, motivated by technology exploration, non-directed (without a specific target in mind) and immediate in their effects. With the rise of personal computers, these early pioneers of hacking started to group in spontaneous associations, espousing discourses of the times on individual freedom, resistance to authority, amusement with detours of emerging technologies. Phreaking and hacking became both shared practices that cemented long friendships between developers, industry pioneers (Wozniak, Jobs, etc.), and politically motivated technology enthusiasts. The borders between an emerging underground culture (yippees, hackers) and a criminal sub-culture were blurry and unstable, with very little self-regulation, and comprising teenagers, advanced computer developers and self-taught technology explorers. We call this era the "code breaking years", where talented

individuals are mostly motivated by symbolic and small gains, a feeling of belonging to a new community and self-identity.

However, in the mid-1980s, technical bulletin boards from hackers' groups started to disclose attack guidelines for intrusions, sometimes both physical and code-based (such as the first issue of the Legion of Doom LOD/H Technical Journal, on Jan. 1, 1987[285]). LOD and MOD (Masters of Deception) hence became influential in transforming these early movements into more organized "cracking" communities, moving a step away from the original hacking culture (see figure 1).

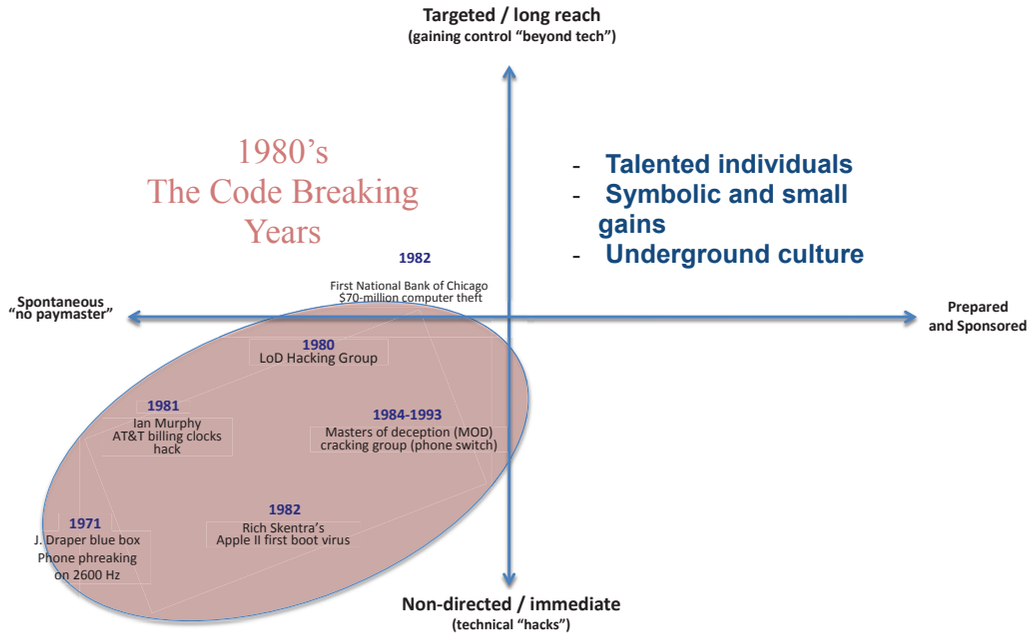


Figure 1: The early years: the code-breaking paradigm

Figure 1: The early years: the code-breaking paradigm

The Cold War and the underground battle for a free Berlin played a determinant role in the evolution of the hacking culture of the late 1980s. The Clifford Stoll episode (a LBL astronomer who accidentally discovered a computer intrusion from West Germany in his laboratory) was the first case to raise the importance of agency coordination and the difficulties of attribution in international computer attacks (Stoll, 1989). This case is also one of the early symptoms (1986) of yet to come advanced persistent threats, highlighting the complexity and sophistication of intrusion campaigns (for details see Stoll's article, 1988[286]). The early 1990s are

[285] http://www.textfiles.com/magazines/LOD/lod-1

[286] http://pdf.textfiles.com/academics/wilyhacker.pdf

hence concomitant with the emergence of criminal sub-culture of hacking. In the 1980s, cracking events that led to theft or large-scale attacks were rare. Two notable exceptions are the 1986 Pak Brain logic bomb, known as the first virus, and the 1982 First National Bank of Chicago computer theft ($70 M USD). The "Great Hacker War" (conflict between Masters of Deception and Legion of Doom, crica 1991-1992) is an example – today disputed as an exaggeration of trivial confrontations – of the interpersonal dynamics of the early 1990s. A blend of prestige-seeking, bravados and playfulness were the core incentives of these early confrontations[287]. The publication of exploits by hackers' groups triggered, however, the interest of Law enforcement. Operation Sundevil, in 1990, was hence the first large-scale cyber-enforcement operation, involving 15 US cities and leading to three arrests[288]. Most cyber-crimes involved wire-tapping, calling card fraud, credit card fraud. The relative failure of this operation led to an increase awareness of the central role of cyber-deterrence for federal agencies (Sterling, 1994).

Publications such as 2600, and the rise of the cyber-space participate to a democratization of cracking, phreaking and hacking techniques, which render them more versatile to their use "beyond technology". Focus on distant control, resident threats (democratization of Trojans) creates both a more organized criminal sub-culture, and the birth of a societal reach for attacks (see figure 2).

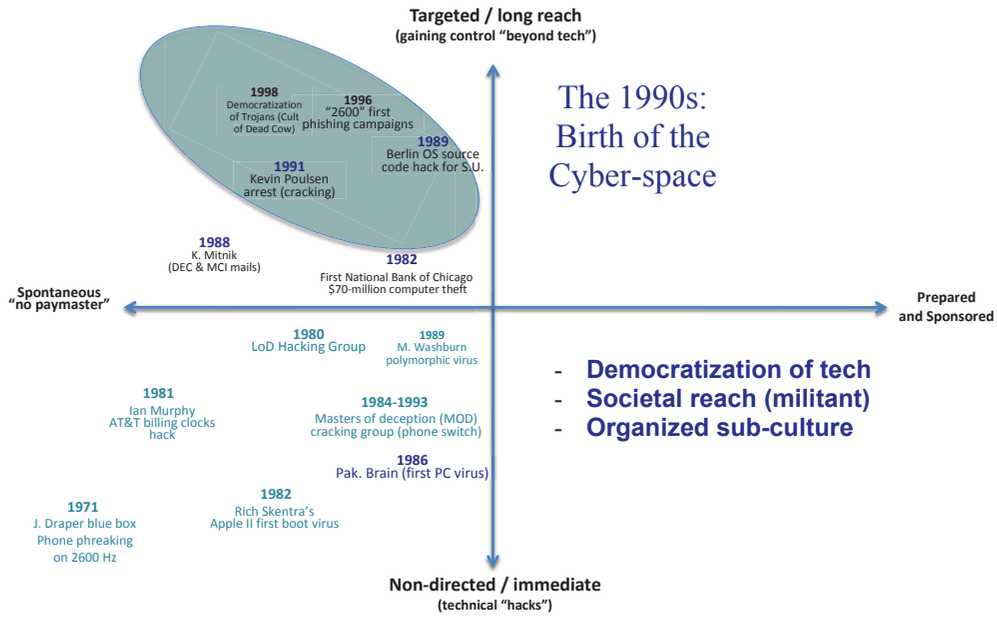


Figure 2: The 1990s: The democratization of cyber-crime

287 http://www.textfiles.com/hacking/modbook4.txt

288 Clapes, Anthony Lawrence (1993). Softwars : the legal battles for control of the global software industry. Westport, Conn.: Quorum Books

While attack preparation is targeted to single point of aggression, the early 2000s is adopting a whole new dynamic. The rise of electronic commerce means a better monetization of cyber-crime with an expectation of large-scale profits for organized crime. The digitalization of the cultural industry (MP3s) creates an appeal for the popular growth of cracking. Profiles of hackers accordingly change in two directions: on one hand, amateur crackers (script kiddies, mass market consumers) start to use without advanced knowledge available tools (P2P file sharing, cracking "CDs"). On the other hand, malware production becomes a profitable black market. Corruption of DNS paths, denial-of-service attacks, defacing campaigns, and corporate thefts find a rapid monetization. The years 2000-2002 are among the most active in malware generation with viruses such as ILOVEYOU, Klez.h., Code Red, etc. The group Anonymous is created in 2003 as a loosely coupled and spontaneous coordination of various interests, ranging from militant activism, cracking techniques sharing, and image sharing around the 4chan platform. Massive raids and pranks, known as "4chan raids", popularize a perspective of hacking as a blend of activism, bullying, and satirist information campaigns, although opting out political campaigns in the early years (2003-2006).

Meanwhile, preparation and sponsorship of large-scale attacks also gain considerable traction as the core philosophy of hacking (based of freedom and activism values) is fading away with the diffusion of embedded cracking tools and libraries. Titan Rain (2003-2006) is an exemplar of these first explorations of cyber-warfare involving low-tech methodologies embedded into advanced campaigns (see Figure 3).

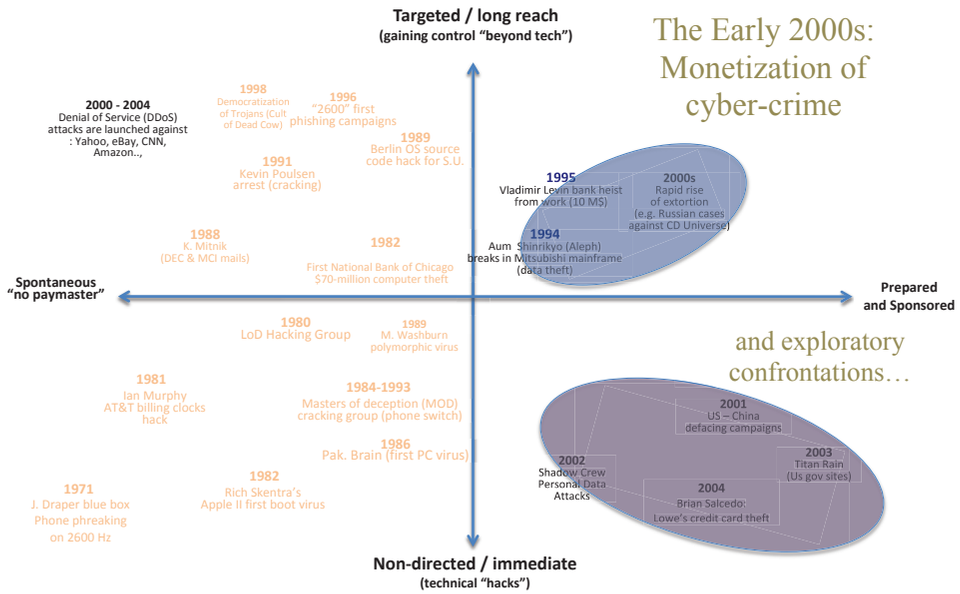


Figure 3: The monetization of cyber-crime and first State confrontations

The years 2005-2013 are marked by a double shift, and in some extent a seizure, between "target and sponsored campaigns" led by States or organized crime, and more pervasive "spontaneous and long-reach campaigns" led by activist groups, hackers' collectives, and loosely coupled entities such as Anonymous and LulzSec. This period is characterized by a rapid growth of strategic and politically motivated attacks (Kerem125 against the United Nations, Chinese APT1 global campaign, Estonia DoS attacks, Stuxnet, Operation Aurora.. Fig. 4).

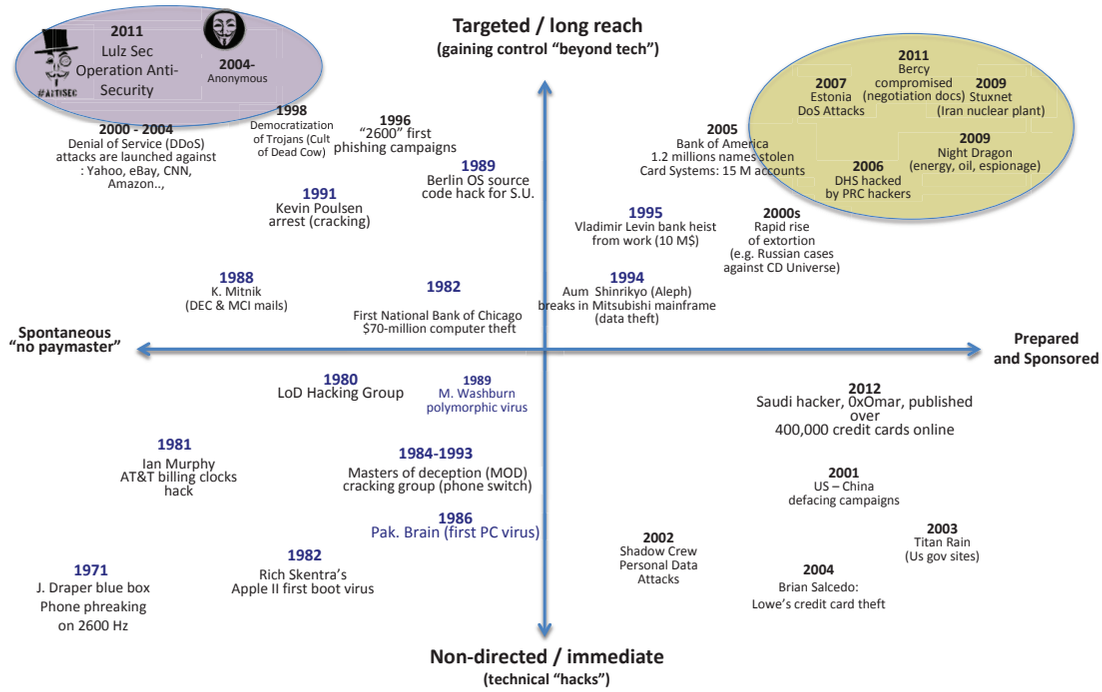


Figure 4: Beyond technology: the rise of large-scale targeted campaigns (2005-2013)

The technology used in these large-scale campaigns does not dramatically differ from the early days of hacking. 125 lines of codes are still very efficient in 2013 to conduct the exploitation of vulnerabilities, even when the lines of defense have exponentially grown in the past 25 years. As most innovation disruptions in the early XXIst century, the performance of these campaigns is rooted in the accessibility and diffusion of combinatory learning, i.e. the capacity of outpacing the defensive learning of targets by a better and faster behavioral intelligence.

The formation of two distinctive groups (large-scale spontaneous groups vs. sponsored targeted large scale campaigns) is typical of the two paths that can be used to attain a superior collective behavioral learning advantage. Large spontaneous groups benefit from distributed astute learning, i.e. the learning conducted by individual hackers who can coordinate on a very large scale, making

their collective learning ubiquitous and efficient. Targeted sponsored campaigns (such as APTs) benefit from the advance of automated artificial intelligence embedded into technology (e.g. Stuxnet, FLAME).

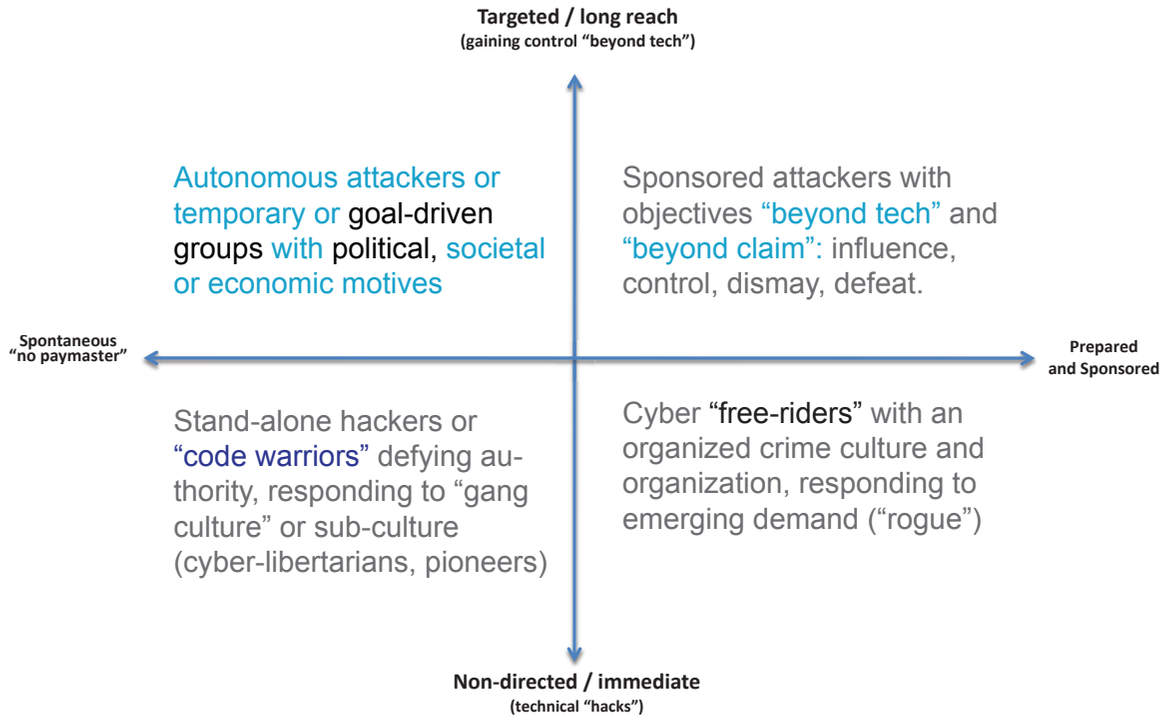
Most defensive systems are based on the recognition of signatures ("embedded malicious codes") of malwares, or on the normative analysis of behaviors compared to "healthy behaviors" (knowledge-based detection systems). Both the collective learning of spontaneous groups, and the signature-based machine learning currently outpace signature-based detection systems. The nature of the current paradigm shift is, in this sense, very similar to the evolution of information warfare in the early 1990s. We are witnessing a strategic disruption where defenders are consolidating their information infrastructures, while attackers are engaging in knowledge-warfare (Baumard, 1994). Superior knowledge, through astute combination, can be gained from truncated and partial information. Superior information rarely defeats even poorly articulated knowledge.

A *behavioral intelligence paradigm* is synonym with an inescapable rise of "zero days" threats. Pervasive and highly available combinatory learning allows the creation of many variants of an exploit (exploitation of a vulnerability) within 24 hours of its discovery. Re-encapsulating and re-combining exploits of undiscovered flaws ("zero days") is made possible by the advancement of causative learning techniques, or when inaccessible, by the very large number of spontaneous hacking groups sharing their recombination experiments. In such a paradigm, focusing on ex-post defense strategy based on known and identified vulnerabilities is likely to fail.

Putting contemporary doctrines to the test of technological shifts

Gathering data from public sources on published Cyber-Defense doctrines, we try in the second part of this analysis to assess the soundness of Cyber-Doctrines for the deterrence of behavioral intelligence-driven threats. We analyzed 38 national strategies to fight cyber-crime, implement cyber-defense, and promote resilient information infrastructures and cyber-security.

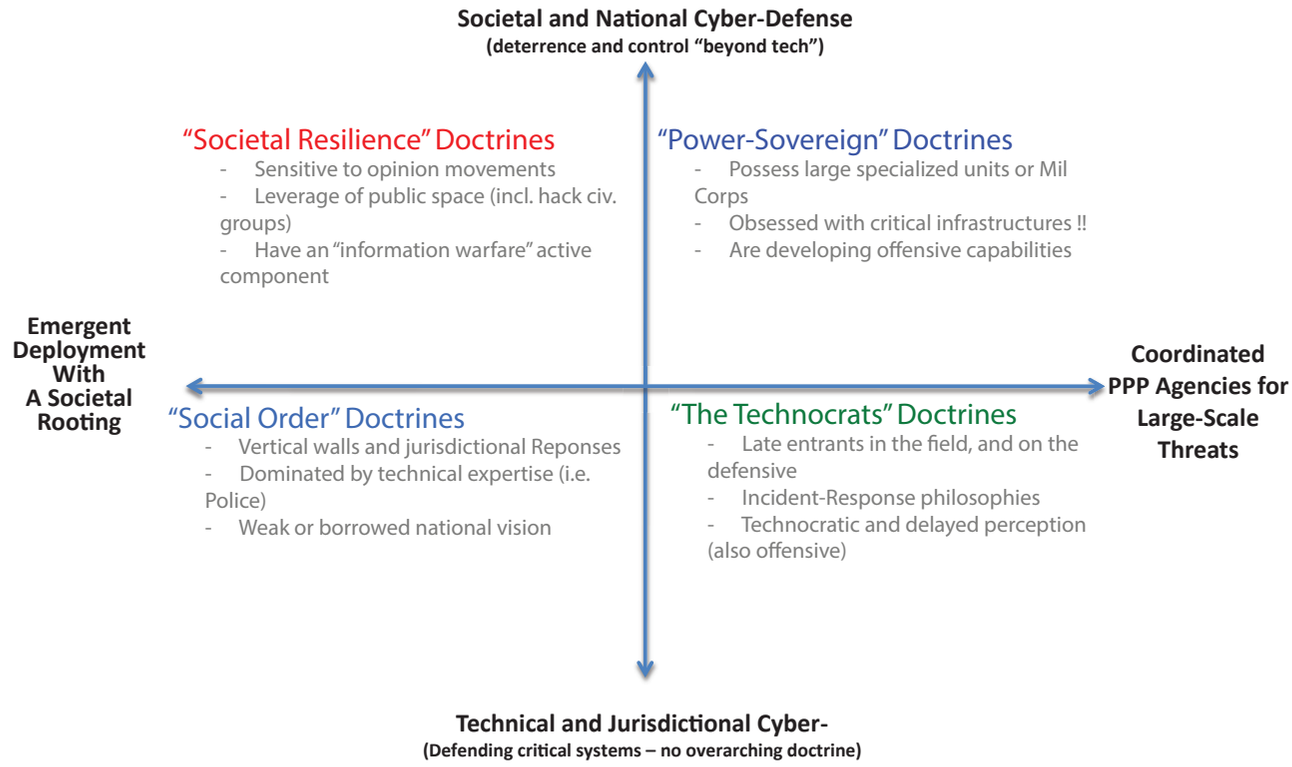
We used the framework developed earlier on the history of cyber-criminality to categorize four categories of Cyber-Crimes, based on their destination ("targeted and long-reach" vs. "immediate or non-directed") and their preparation ("spontaneous" vs. "prepared and sponsored"). Hence, we identify four classes of cyber-crime: "code warriors" (I), "cyber free riders" (II), "autonomous collectives" (III) and "sponsored attackers" (IV).



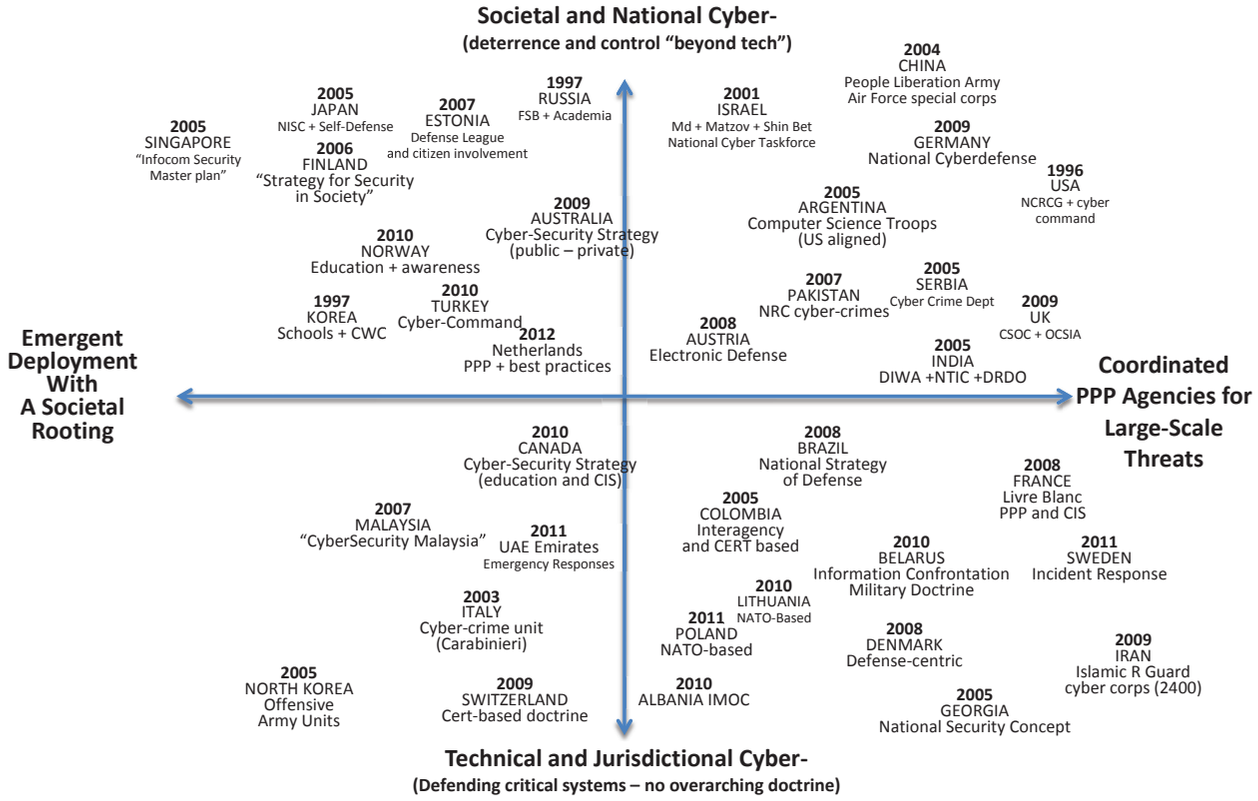
Different classes of attacks require different responses. Immediate and spontaneous attacks (Class I) can be handled with robust information security, including causative learning that can deter sophisticated AI attacks. Most national doctrines have a sound understanding and appropriate range of responses for such attacks. Prepared and sponsored immediate attacks (computer theft by organize crime, free-riding, phishing and cracking – Class II) require a coordinated range of technical and jurisdictional responses. Signature-based detection systems and knowledge-based defenses are usually sufficient to deter most threats, as far as regulation is judicially enforced. Socially and society-rooted attacks (hactivist groups, temporary of goal-driven groups with political, societal or economic motives - Class III) involves perception warfare, information warfare, sense-making capabilities as to respond to rapid and emergent distributed deployment. Finally, offensive campaigns with embedded behavioral intelligence (Class IV) require transversal responses that encompass proactive deterrence "beyond tech" and "beyond claim". Class III and Class IV threats call for real-time sense-making on unprecedented scales, involving large-scale human cognitive learning on one side (III) and large-scale behavioral learning on the other side (IV).

Our analysis of the evolution of national cyber-crime doctrines over the period 1994-2013 brings mixed findings. *"Power-sovereign" doctrines* (P-S, Class IV) emphasize the development of large specialized units, are often obsessed with

critical infrastructures protection, and develop more or less publicly, offensive capabilities. While they deliver sustainable deterrence policies on State-sponsored cyber attacks, they usually develop a threat-rigidity dominant logic, which impedes their involvement in emergent societal change. The risk for P-S doctrines is therefore disconnecting with emergent hacking movements, and a lack of reactivity to distributed cognitive warfare. *"Societal Resilience"* doctrines (Class III), on the other hand, are more sensitive to opinion movements, try to leverage the public space, and focus their offensive capabilities on information warfare. Motivation for such doctrines is not always rooted in a democratic and progressive view of the Internet. Yet, the digitalization of society is clearly identified as both the core threat and core opportunity for cyber-defense and cyber-development. Finally, "Social order" doctrines (Class I) and "Technocratic" doctrines (Class II) only differ in their perception of control. The main difference lies in a control at the source (I) vs. a control by a normalization of the outputs (II). Technocratic perspectives often suffer from a delayed perception of technological change, mainly inspired by an incident-response philosophy or a late entry to the field. Doctrines that favor social order generally suffer from a lack of national vision or national strategy, or have built their policies by borrowing (or aligning to) external national visions.



The following graph presents the positioning of different national cyber-crime deterrence and cyber-defense strategies (year indicates date of first document analyzed). Findings illustrate the trade-off between national policies that focused on organized cyber-crime and policies driven by the surveillance (or the support) of the societal rooting of cyber-developments. Interestingly, the Russian cyber-doctrine is closer to emergent societal developments than its Chinese or US counterparts.



Measuring the robustness of national strategies: what to expect?

Most of the studied national strategies derive their national cyber criminality deterrence with an average delay of 10 to 15 years with the advancement of technology. Accordingly, society-wide disruptions have been systematically overlooked. Typically, cyber-policies grow in the fourth class, while the most disruptive change is taking place in the third.

Core hacking technologies have been steadily stable in the 1990-2012 period. Advanced Persistent Threats (APTs) are per se the result of a disruption in core exploits, but rather a paradigmatic change coming from peripheral technologies (mainly: machine learning, automation, combinatory reconfiguration). Such a paradigmatic change thrives on the obsolescence of an aging infrastructure.

Combinations are made possible when flaws can be exploited cross-systems. The growing interoperability of vulnerable systems increases the probability of the on-the-fly exploitation of cross-vulnerabilities. In such a context, vendors, by pushing cyber-criminality deterrence to focus on "points of access" vulnerability assessment impedes the investment in behavioral learning technologies (by maintaining a poorly performing, but highly profitable, signature-based defense paradigm).

The only way to counter-act and deter intelligent behaviors is by outpacing and outsmarting its behavioral intelligence. Very few studied doctrines have acknowledged this core systemic vulnerability. Confidence building and security measures (CBSMs) are hence rooted in a technological and societal understanding that may foster vulnerabilities, and suffer from a critical blind spot on the nature of future technological threats.

Technocratic (Class II) and social order (Class I) national doctrines are dependent on vertical and jurisdictional knowledge, while the evolution of threats is horizontal and a-jurisdictional. Most recent large-scale campaigns (APT1, Blaster-worm, etc) have shown the limits of inter-jurisdictional coordination in responding to attacks with unpredictable attribution, unknown or undiscovered signatures, and using causative learning to adapt to common technical responses.

Most of the analyzed doctrines presented an outdated perception of authorship and attribution. Attribution is assimilated in most doctrines with a geographical point of emission (or several), a central intent, and a legalist perspective on tracking back attacks. Erasing traces of presence, or traces of intrusion, has been long mastered by the hacking community, leading to the conclusion that diplomatic efforts are geared towards resolving an issue that has lost its technological pertinence before 2007.

Understanding the social psychology of threats development is becoming critical, as we are entering a pioneering period that strangely resembles of the "phreaking" years of hacking (1972-1987). The improved portability of machine learning (embarked, distributed or fully autonomous) is curiously absent from most national strategies' assumptions. This may be driven by the transposition of the principles of military capabilities escalation (weapons race, concentration, decisive capacities) to the tackling of cyber-criminality. Cybernetic offensive capabilities do not respond to traditional escalation and reinforcement models. They derive their malevolent capabilities from their transformational nature, their distributed deployment, and their superior and autonomous learning.

References

1. Barreno Marco, Peter L. Bartlett, Fuching Jack Chi, Anthony D. Joseph, Blaine Nelson, Benjamin I. P. Rubinstein, Udam Saini, and J. D. Tygar (2008), "Open Problems in the Security of Learning", *First ACM Workshop on Security and Artificial Intelligence (AISec)*, pp. 19-26, Alexandria, Virginia.

2. Baumard, P. (1994), «From Information Warfare to Knowledge Warfare: », in : W. Schwartau (Ed.) (1994), *Information warfare*, New York : Thunder's Mouth Press, pp. 611-626

3. Bodmer, Kilger, Carpenter, & Jones (2012). Reverse Deception: Organized Cyber Threat Counter-Exploitation. New York: McGraw-Hill Osborne Media.

4. Gaycken, Sandro (2012) "Die sieben Plagen des Cyberwar," In R Schmidt-Radefeldt & C Meissler, C. (eds.), *Automatisierung und Digitalisierung des Krieges*, Berlin: Forum Innere Führung.

5. Rubinstein Benjamin I. P., Blaine Nelson, Ling Huang, Anthony D. Joseph, Shing-hon Lau, Satish Rao, Nina Taft, and J. D. Tygar, (2009), "ANTIDOTE: Understanding and Defending against Poisoning of Anomaly Detectors", *IMC '09: Proceedings of the 9th ACM SIGCOMM on Internet Measurement Conference*, pp. 1-14, Chicago, IL.

6. Sterling, Bruce (1994). «Part Three: Law and Order». The Hacker Crackdown: Law And Disorder On The Electronic Frontier. New York: Bantam Books.

7. Stoll, Cliff (1988), "Stalking the wily hacker", *Communications of the ACM*, 31(5), pp. 484-500.

8. Stoll, Cliff (1989), The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, New-York: DoubleBay.

Карасев П.А.
Институт проблем информационной
безопасности МГУ имени М.В.Ломоносова

ОБЗОР НАЦИОНАЛЬНЫХ ПОДХОДОВ К ПРОБЛЕМЕ ФИЛЬТРАЦИИ КОНТЕНТА В ИНТЕРНЕТЕ

Интернет как глобальный феномен, состоящий из различных устройств, проводных и беспроводных сетей, сегодня стал местом, где создаётся, передаётся и хранится гигантский объём информации. При этом те, кто создают контент, руководствуются самыми разными целями, в том числе и деструктивными.

Сегодня пользователь Интернета, погружаясь в бесконечный поток информации, зачастую не может в полной мере воспринять и осознать потребляемый контент, а вместе с этим – не может в полной мере оценить его влияние на свою психику и поведение. Кроме того, пользователи социальных сетей и иных сервисов, позволяющих размещать в Интернете различный контент, часто не отдают себе отчет в том, что, выкладывая на всеобщее обозрение информацию о себе, они уже не смогут бесследно удалить её. Конфиденциальная информация или личные данные могут оказаться в руках злоумышленников, которые станут использовать её по своему усмотрению. Особой опасности в этом отношении подвергаются несовершеннолетние.

Необходимым условием ограничения разрушительного воздействия информации представляется наличие некоторых разумных ограничений, например цензурных, реализуемых в той или иной форме через прозрачные механизмы, при наличии общественного контроля над их деятельностью.

Как говорится в пункте 2 статьи 29 «Всеобщей декларации прав человека», «при осуществлении своих прав и свобод каждый человек должен подвергаться только таким ограничениям, какие установлены законом исключительно с целью обеспечения должного признания и уважения прав и

свобод других и удовлетворения справедливых требований морали, общественного порядка и общего благосостояния в демократическом обществе». В статье 19 Международного пакта о гражданских и политических правах, говорится об ограничениях при реализации прав человека: а) для уважения прав и репутации других лиц; б) для охраны государственной безопасности, общественного порядка, здоровья или нравственности населения.

На первый план выдвигается необходимость соблюдения баланса между правами и свободами Интернет-пользователей и обеспечением безопасности в информационной среде (киберпространстве). Мы должны признать, что каждый имеет право на защиту от контента, который он считает вредоносным для себя, своей семьи, своего общества. При этом, важно сохранить весь позитивный потенциал информационно-коммуникационных технологий. Многие государства мира, в том числе и развитые западные демократии уже осознали эту проблему и выработали свои механизмы признания определенного контента вредоносным и механизмы защиты от него.

Продемонстрируем на примерах, контент какого характера запрещен к распространению, подвергается фильтрации тем, или иным образом. В настоящем обзоре выделено несколько видов фильтруемого контента:

1. Дискриминационный контент и клевета;
2. Контент, фильтруемый для защиты молодёжи;
3. Контент, фильтруемый по социально-культурным критериям и в интересах общественной безопасности.

1. Дискриминационный контент и клевета

Начать следует с упоминания 2 статьи Всеобщей декларации прав человека, которая говорит о том, что «каждый человек должен обладать всеми правами и всеми свободами, провозглашенными Декларацией, без какого бы то ни было различия, как то в отношении расы, цвета кожи, пола, языка, религии, политических или иных убеждений, национального или социального происхождения, имущественного, сословного или иного положения».

В протоколе к Будапештской Конвенции по киберпреступности Совета Европы, от государств-подписантов требуется «предпринимать шаги по криминализации контента в текстовой, визуальной или иной форме, который оправдывает, поощряет или вызывает ненависть, дискриминацию или насилие, направленных против индивида или группы лиц, на основании расы, цвета кожи, происхождения или религии».

Статья 320.1 уголовного кодекса Канады устанавливает уголовную ответственность за контент, разжигающий ненависть по различным критериям.

Закон Индонезии «Об информации и электронных транзакциях» 2008 года запрещает клевету, а также контент, направленный на разжигание ненависти или враждебности по отношению к человеку или группе лиц, на основании их расы, этнической принадлежности и религии.

2. Безусловно преступной признана детская порнография, и многие государства, в том числе Великобритания, Швеция, Финляндия, Дания, Германия, Франция и Италия осуществляют фильтрацию сайтов, содержащих такой контент, используя сеть «горячих линий», от которых информация о вредоносном контенте передаётся Интернет-провайдерам для последующего включения в черные списки. Также огромное значение приобретает задача защиты детей от вредоносной информации в Интернете.

В 2006 году Национальная ассамблея Венесуэлы приняла закон «О защите детей от вредного контента в Интернете». Согласно этому закону, провайдеры обязаны не только следить за контентом на своих серверах, но и предоставлять пользователям программное обеспечение для фильтрации контента.

3. Определенный контент в ряде государств считается угрозой национальной безопасности. Кроме того, ряд государств сталкивается с проблемой эрозии традиционных ценностей, культурной и моральной составляющей общества, а также с контентом, который неприемлем в определенной социально-культурной среде.

В 2009 году Парламентом Индии принято дополнение к закону «Об информационных технологиях», которое расширило права правительства по блокировке вебсайтов, считающихся угрозой национальной безопасности.

В 2010 году правительство КНР внесло дополнения в закон «О государственной тайне», предписывающий Интернет-провайдерам сотрудничать с государством в случае обнаружения утечек государственных секретов в Интернет.

В Венесуэле закон «О социальной ответственности Радио и телевидения» с поправками 2010 года регламентирует ответственность и запрещает контент, в том числе размещенный в Интернете, направленный на подрыв общественного порядка или побуждение действий, угрожающих национальной безопасности.

Опасным признаётся контент террористической и экстремистской направленности. В 2003 году в Кении был принят закон «О противодействии терроризму», согласно которому запрещены «сбор, создание и передача информации (в том числе онлайн), полезной для террористических организаций».

В ОАЭ законом «О киберпреступлениях» 2006 года запрещено размещение контента оскверняющего святыни или религиозные обряды, противодействующего исламу, направленного на отрицание семейных ценностей и принципов, нарушающего общественный порядок, продвигающего идеологию терроризма. Закон «О киберпреступлениях» криминализует создание вебсайтов, направленных на продвижение идеологии терроризма, финансирование терроризма, и распространение инструкций по изготовлению взрывчатых веществ.

В Южной Корее закон «О сфере телекоммуникаций» запрещает распространение информации, «нарушающей общественный порядок, или мо-ральные нормы и традиции».

В Новой Зеландии, в соответствии с законом «О классификации фильмов, видеоматериалов и публикаций», запрещено распространять или обладать таким материалом, который считается «вредным для общественного блага».

Статья 57 закона Бангладеш «Об Информационно-коммуникационных технологиях» 2006 года запрещает «вульгарный, клеветнический» и «оскорбляющий религиозные чувства» контент.

Статья 211 закона Малайзии «О коммуникациях и мультимедиа» 1998 года запрещает размещение в сети контента, «являющегося непристойным, нецензурным, клеветническим или содержащим угрозы».

В Российской Федерации также принят ряд законов, регулирующих вопросы фильтрации некоторых категорий контента. 28 июля 2012 года вступил в силу закон № 139-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные акты Российской Федерации». В Федеральный закон № 436-ФЗ от 29 февраля 2010 года «О защите детей от информации, причиняющей вред их здоровью и развитию» были внесены следующие существенные изменения. Прежде всего, в закон внесли требование об обязательном размещении на информационной продукции знака, указывающего категорию информационной продукции. При этом информационная продукция подлежит экспертизе в порядке, установленном законом.

Закон № 126-ФЗ от 7 июля 2003 года «О связи» был дополнен пунктом, согласно которому «оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», обязан осуществлять ограничение и возобновление доступа к информации, распространяемой посредством информационно-телекоммуникационной

сети «Интернет», в порядке, установленном Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Изменения затронули и федеральный закон №149-ФЗ «Об информации, информационных технологиях и о защите информации». В него было введено положение о создании единого реестра сайтов в сети Интернет в целях ограничения доступа к размещенному на этих сайтах вредоносному контенту. Установлено, что в реестр включаются материалы в соответствии с решениями полномочного органа федеральной власти – Роскомнадзора, или в соответствии с решением суда.

В компетенцию суда входит принятие решений по любой категории контента, запрещенного к распространению на территории Российской Федерации. В соответствии с федеральным законом №114-ФЗ «О противодействии экстремистской деятельности» от 25 июля 2002 года (в редакции 2008 года), запрещено распространение экстремистских материалов, а также их производство или хранение в целях распространения. Закон N 2124-1 «О средствах массовой информации» от 27 декабря 1991 года (в редакции 28.07.2012) запрещает разглашение сведений, составляющих государственную или иную специально охраняемую законом тайну, распространение материалов, содержащих публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов, а также материалов, пропагандирующих порнографию, культ насилия и жестокости.

Интернет должен, несомненно, оставаться пространством свободы и общечеловеческим достоянием; каждый должен обладать правом на доступ к информации и правом на свободу самовыражения. Статья 19 «Всеобщей декларации прав человека» гласит: «Каждый человек имеет право на свободу убеждений и на свободное выражение их; это право включает свободу беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ».

В то же время нельзя отрицать тот факт, что свобода не подразумевает вседозволенность, а, напротив, подразумевает ответственность за свои действия – как в физическом мире, так и виртуальном пространстве. Абсолютная свобода распространения информации сделала бы совместную жизнь людей невозможной.

По результатам дискуссий во время Шестой и Седьмой конференций Международного исследовательского консорциума информационной безопасности составлена следующая таблица.

Сводная таблица, отображающая подходы государств и основные законодательные акты, регламентирующие фильтрацию вредоносного Интернет-контента

Страна	Законодательная база	Фильтруемые ресурсы	Регулирующие органы	Механизм фильтрации
Россия	Федеральный закон № 139-ФЗ от 28 июля 2012 года «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные акты Российской Федерации»	- Материалы с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера; - Информация о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, местах приобретения таких средств, веществ и их прекурсоров, о способах и местах культивирования наркосодержащих растений; - Информация о способах совершения самоубийства, а также призывов к совершению самоубийства.	Роскомнадзор	Создан единый реестр сайтов в сети Интернет в целях ограничения доступа к размещенному на этих сайтах вредоносному контенту. В реестр включаются материалы в соответствии с решениями полномочного органа федеральной власти – Роскомнадзора, или в соответствии с решением суда

Канада	Статья 320.1 уголовного кодекса Канады	Контент, разжигающий ненависть по различным критериям.	Комиссия по Радио, Телевидению и Телекоммуникациям, проект Cleanfeed	Удаление материалов через суд. Блокирование и удаление контента на уровне Интернет-провайдеров.
	Статья 163 уголовного кодекса Канады	Детская порнография		
Венесуэла	Закон 2006 года «О защите детей от вредного контента в Интернете».	Материалы, вредные для несовершеннолетних.		Блокирование и удаление контента на уровне Интернет-провайдеров, предоставление средств фильтрации пользователям.
	Закон 2004 года о социальной ответственности СМИ (с изменениями от 2010 года)	Материалы, направленные на нарушение общественного порядка и опасные для национальной безопасности		
Кения	Закон 2003 года «О противодействии терроризму»	«Информация, которая может быть полезна террористам»		
Бангладеш	Закон «О Информационно-коммуникационных технологиях»	«Вульгарный, клеветнический» и «оскорбляющий религиозные чувства» контент.		
	Закон «О контроле порнографии»	Порнография, материалы, вредные для несовершеннолетних		

Индонезия	Закон «Об электронной передаче информации и транзакциях»	Клевета, информация, направленная на разжигание розни по расовому, этническому и религиозному признаку.	Министерство связи и информационных технологий	
	Закон №44 от 2008 года «О порнографии»	Порнография		
Южная Корея	Закон «О сфере телекоммуникаций» (TELECOMMUNICATIONS BUSINESS ACT) с изменениями и дополнениями, внесенными законом №8867 от 29 февраля 2008 года	Информация, «нарушающая общественный порядок, или моральные нормы и традиции»	Комиссия по телекоммуникациями Кореи	Блокирование и удаление контента на уровне Интернет-провайдеров
	Закон «О защите молодежи»	Материалы, вредные для несовершеннолетних.		
	Закон «О защите молодежи от сексуальной эксплуатации»	Детская порнография		
Малайзия	Закон «О связи и мультимедиа»	Контент, «являющийся непристойным, нецензурным, клеветническим или содержащим угрозы»		

Бразилия	Закон 1967 года «О печати»	Клевета	Национальный центр сообщений о компьютерных преступлениях, Федеральная прокуратура Бразилии	Блокирование и удаление контента на уровне Интернет-провайдеров
	Закон 2003 года «О борьбе с детской порнографией»	Детская порнография		
Оман	Статья 29 Конституции Омана 1984 года «О прессе и публикациях» Условия использования сетей Omantel	Контент, который считается политически, культурно или оскорбительным		
ОАЭ	Закон 2006 года «О киберпреступле-ниях»	Контент, оскверняющий святыни или религиозные обряды, противодействующий исламу, направленный на отрицание семейных ценностей и принципов, нарушающий общественный порядок, продвигающий идеологию терроризма.	Министерство Юстиции, Исламских дел и Вакуфов	

Алжир	Декрет о телекоммуникациях	Контент, считающийся «аморальным и нарушающим общественный порядок»		Блокирование и удаление контента на уровне Интернет-провайдеров
Австралия	Закон 1999 года «О дополнительном регулировании услуг связи» Закон 1975 года «О расовой дискриминации»	Контент, цель которого «оскорбить, унизить или запугать другого человека (группу лиц) на основании их расы, цвета кожи, или происхождения»	Агентство связи и массовой информации Австралии	Блокирование и фильтрование контента по решению суда. В 2006 году правительство Австралии запустило программу по «Защите австралийских семей онлайн». В рамках этой программы семьи получат бесплатные интернет-фильтры.
Новая Зеландия	Закон «О классификации фильмов, видеоматериалов и публикаций»	Контент, считающийся «вредным для общественного блага»	Министерство Внутренних дел Новой Зеландии	

Индия	Закон «Об информацион-ных технологиях»	Контент, считающийся угрозой национальной безопасности и общественному порядку		
США		Из поправки о свободе слова исключаются: Непристойный контент; Некоторые виды обнаженной натуры; Детская порнография; Подстрекательство к насилию или противоправным действиям; Ограничения в военное время или в чрезвычайных ситуациях; Ограничения для участников судебного процесса; Клевета; Ложная реклама.	Суды	Блокирование и фильтрование контента по решению суда. Самоцензура.

Япония	Закон «О защите молодежи в Интернет-пространстве»	Материалы, вредные для несовершеннолетних: провоцирующие правонарушения; информация о суициде; Жестокость; Непристойности.		Требования в законе не подкреплены санкциями
	Расширение применения существующих законов	Терроризм, подстрекательство к войне или беспорядкам, религиозный экстремизм, Интернет-мошенничество.		

P.A.Karasev
Institute of Information Security Issues,
Lomonosov Moscow State University

OVERVIEW OF NATIONAL APPROACHES TO CONTENT FILTRATION IN THE INTERNET

The Internet as a global phenomenon composed of different hardware devices, wired and wireless networks has become a domain where a huge amount of information is being created, transmitted and stored. People who create the content, however, pursue a variety of goals including destructive ones.

Today Internet users as they submerge themselves into an endless flow of information often cannot fully perceive and understand consumed content, and consequently are unable to fully assess its impact on their minds and behavior. Furthermore, users of social networks and other services that allow to upload various content are often unaware of the fact that once they have uploaded their personal data for public use they will never be able to delete it completely. Thus, confidential information or personal data can end up in the hands of criminals who might use it to their advantage. Minors are especially vulnerable to such threat.

The essential prerequisite to prevent the impact of «destructive» information is to establish certain reasonable safeguards such as censorship, which could be implemented in one form or another through transparent mechanisms, provided there are under public control.

Paragraph 2, Article 29 of the Universal Declaration of Human Rights states: «In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.» Article 19 of the International Covenant on Civil and Political Rights sets forth restrictions to human rights as follows: a) For respect of the rights or reputations of others, and b) for the protection of national security or of public order, health or morals.

The first priority in this issue is to maintain the balance between the rights and freedoms of Internet users and security of the information space (cyberspace). We must recognize that every person has the right for protection from the content that he/she deems harmful for himself/herself or his/her family or the society as a

whole. At the same time we must preserve all the positive potential of information and communication technologies. Many countries of the world, including developed Western democracies, have recognized this problem and developed their own frameworks to classify certain content as harmful and methods of protection against such content.

Below there are examples of the content which is prohibited for distribution or filtered in one way or another. This review recognizes several types of content subject to filtering:

1. Discrimination and Defamation;

2. Content filtered to protect the youth

3. Content, filtered by Social or Cultural criteria, and seen as Contrary to Public Order and National Security.

1. Discrimination and Defamation

We should begin with Article 2 of the Universal Declaration of Human Rights which states that "everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, color, sex, language, religion, political or other opinion, national or social origin, property, birth or other status."

The protocol to the Council of Europe Budapest Convention on Cybercrime requires the signatory states to "take steps to criminalize the content in a text or visual form or otherwise that justifies, encourages or causes hatred, discrimination or violence against an individual or a group of individuals based on his/her or their race, color, origin or religion."

Section 320.1 of the Canadian Criminal Code makes dissemination of online hate propaganda a criminal offense.

The Indonesian law on information and electronic transactions of 2008 prohibits defamation and any content inciting hatred or hostility towards a person or group of people in view of his/her or their race, ethnicity or religion.

2. Child pornography is unconditionally recognized as crime and many states, including the United Kingdom, Sweden, Finland, Denmark, Germany, France and Italy filter websites offering such content by using a network of "hotlines" which pass data on harmful content to ISPs who then blacklist such websites. Another important challenge of the present day is to protect children from harmful information they might find on the Internet.

In 2006 the National Assembly of Venezuelan adopted a law concerning protection of children from harmful Internet content. Under the law, internet

providers are required not only to monitor the content stored on their servers, but also provide users with content-filtering software.

3. In a number of countries certain types of content are considered a threat to national security. Today a number of nations face the problem of erosion of traditional values which make the cultural and moral foundation of the society. Certain Internet content may be unacceptable in a particular socio-cultural environment.

In 2009 the Indian Parliament amended the law regulating information technologies and gave the government broader rights to block websites considered a threat to national security.

In 2010 the Chinese government amended the State Secrets Act that now requires cooperation of Internet service providers with the state whenever a state secret leaks to the Internet.

Venezuelan law on social responsibility on radio and television as amended in 2010 establishes responsibility and prohibits content, including Internet content, which aims to undermine public peace or induce actions posing a threat to national security.

Content related to terrorism or extremism is also recognized as dangerous. In 2003 Kenya passed Terrorism Act which prohibits "to collect, create and transfer (including via the Internet) information useful for terrorist organizations."

The UAE Cybercrime Act (2006) prohibits content desecrating objects of worship or religious ceremonies, content in opposition to the teaching of Islam, content denying family values and principles, or content disturbing public peace or promoting the ideology of terrorism. The Law of 2006 criminalizes creation of websites promoting the ideology of terrorism, financing terrorist activities and spreading instructions on how to manufacture of explosives.

The South Korean Telecommunications Business Act prohibits dissemination of Content that violates the honor or rights of other persons or undermines public morals or social ethics.

Under the Films, Videos, and Publications Classification Act of New Zealand it is prohibited to distribute or possess materials considered to be "detrimental to the public good."

Article 57 of the Bangladesh Information and Communication Technologies Act (2006) prohibits content that is "vulgar, slanderous or offending religious feelings".

Article 211 of the Malaysian Communications and Multimedia Act (1998) prohibits posting on the Internet any content which is "indecent, obscene, defamatory or threating."

The Russian Federation has also adopted a number of laws governing filtering of certain categories of content. On July 28, 2012 the Federal Law No. 139-FZ *On Amending the Federal Law "On Protection of Children from Information Detrimental to Their Health and Development" and Other Legal Acts of the Russian Federation* was adopted. The following significant changes were introduced into the Federal Law No. 436-FZ of February 29, 2010 *On Protection of Children from Information Detrimental to Their Health and Development.*

First and foremost, the law now requires an information product to be marked with a sign identifying the category of such information product, while information products themselves are now required to undergo an expert review in the manner prescribed by law.

The Federal Law No. 126-FZ of July 7, 2003 *On Telecommunication* was amended with a paragraph stating that "telecommunication operators who provide access to the information and telecommunication network "the Internet" are required to restrict and resume access to the information disseminated through the information and telecommunication network «the Internet» as regulated by the Federal Law No. 149-FZ of July 27, 2006 *On Information, Information Technologies and Protection of Information.*

The Federal Law No. 149-FZ *On Information, Information Technologies and Protection of Information* has also been amended. Now it requires that a unified website register is maintained with the purpose of restricting access to harmful content posted on certain websites. Websites are added to the register subject to a decision taken by a competent federal authority (the Federal Supervision Agency for Information Technologies and Communications, *Roskomnadzor*) or under a court ruling.

The jurisdiction of courts includes rulings on any category of content prohibited for distribution in the territory of the Russian Federation. The Federal Law No. 114-FZ *On Countering Extremist Activities* of July 25, 2002 (as amended in 2008) prohibits distribution of extremist materials, as well as their production or storage for the purposes of distribution. The Law No. 2124-1 of December 27, 1991 *On Mass Media* (as amended on July 28, 2012) prohibits disclosure of any information constituting a state secret or other secrets protected by law, distribution of materials containing public calls for terrorism or public justification of terrorism and other extremist materials, as well as materials promoting pornography, violence and cruelty.

The Internet must undoubtedly remain a space of freedom and common heritage of the mankind; everyone must have the right to access information and the right to freedom of expression. Article 19 of the Universal Declaration of Human

Rights states that "everyone has the right to freedom of opinion and expression: this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

At the same it must be remembered that freedom does not mean total permissiveness, but rather means responsibility for the actions one undertakes both in the physical reality and within the virtual space. Absolute freedom to disseminate any information would have rendered joint residence of people impossible.

The table below results from the discussions at the Sixth and Seventh Conference of the International Information Security Research Consortium (IISRC).

Summary table illustrating approaches exercised by various countries and respective legislative instruments governing the filtering of harmful Internet content

Country	Legal framework	Filtered content	Regulating authority	Filtration framework
Russia	Federal law of Russian Federation no. 139-FZ of 2012-07-28 «On Amendments to Federal Law On Protecting Children from Information Harmful to Their Health and Development and Certain Legislative Acts of the Russian Federation.»	• Child pornography or solicitation to participate in such; • Information about methods of making, using, getting or locating narcotic drugs and psychotropic substances or their precursors; or growing plants containing narcotic substances; • Information about methods of suicide, and calls for suicide	Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (ROSKOMNADZOR)	In order to limit access to websites containing information whose dissemination is prohibited in the Russian Federation, the federal law provides for the establishment of a Unified Register of Domain Names, Universal Page Selectors and Internet Addresses that Allow for the Identification of Websites Containing Information whose Dissemination is Prohibited in the Russian Federation. The websites would be included into the Registry based on decisions made by Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications, or by ruling of the court.

Canada	Section 320.1 of the Canadian Criminal Code	Online hate propaganda	Canadian Radio-Television and Telecommunications Commission Project Cleanfeed Canada	Removal and blocking of content by a court order
	Section 163 of the Canadian Criminal Code	Child pornography		
Venezuela	Venezuela's 2004 Law of Social Responsibility for Radio and Television (LSR) (amended in 2010)	Content intended to adversely affect public order or promote crime; or incite actions detrimental to Venezuela's national security	The Municipal Council of Children's Rights	
	Ley para la Proteccion del Nino y Adolescentes en Salas de Uso de Internet Videojuegos y Otros Multimedias	Content, harmful to youth		
Kenya	The Kenya Communications (Amendment) Act 2009	Content, harmful to youth	Communications Commission of Kenya	
Bangladesh	Article 57 of the Information and Communication and Technologies Act	Defamatory content, content that may harm law and order, and content that attacks religious beliefs		
	Pornography Control Act 2011	Pornography Content, harmful to youth		

Indonesia	Law of the Republic of Indonesia Number 11 Year 2008, About Information and Electronic Transactions	Defamatory content Content intended to invoke hatred or hostility toward individuals or groups of people based on race, ethnicity, and religion	Ministry of Communications and Information Technology	
	Law of the Republic of Indonesia Number 44 Year 2008 about Pornography	Pornography		
South Korea	Constitution of Korea Article 21 TELECOMMUNICATIONS BUSINESS ACT with Amendment №8867,Year 2008	Content that violates the honor or rights of other persons or undermines public morals or social ethics Content that aims at or abets a criminal act, aims at committing antistate activities, or impedes good customs and other aspects of social order	Ministry of Information and Communication Korean Communications Standards Commission National Election Commission	Removal and blocking of content by a court order at ISPs
	Juvenile Protection Act	Content, harmful to youth		
	Act on Protection of Youth from Sexual Exploitation	Child pornography		

Malaysia	Communications and Multimedia Act of 1998 Section 211	Online content that is indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass any person.	Malaysian Communications and Multimedia Commission	
Brazil	Press Law # 5.250/67, Article 75	Defamatory content	National Reporting Center of Cyber Crimes Public Ministry	Removal and blocking of content by a court order at ISPs
	Law# 11.829/2008 on Child Pornography on the Internet	Child pornography		
Oman	Article 29 of Oman's constitution 1984 Press and Publication Law Omantel's Terms and Conditions	Content that leads to public discord, violates the security of the State or abuses a person's dignity and his rights		
The UAE	Cyber-Crime Law No. 2 of 2006	Content that defames Islamic places of worship and traditions, insults any recognized religion, or promotes «sinful acts».	Telecommunication Regulatory Authority	Removal and blocking of content at ISPs
Algeria	Article 14 of a 1998 Telecommunications decree	Material contrary to public order and morality		Removal and blocking of content at ISPs

Матюхин В.Г.,
Научный руководитель,
Научно-исследовательский
и проектно-конструкторский
институт информатизации,
автоматизации и связи
на железнодорожном транспорте

ТРАНСГРАНИЧНЫЙ ЮРИДИЧЕСКИ ЗНАЧИМЫЙ ДОКУМЕНТООБОРОТ В ОАО «РЖД»

В соответствии со «Стратегией развития железнодорожного транспорта в Российской Федерации до 2030 года» одним из приоритетных направлений транспортной политики Российской Федерации является создание эффективных, безопасных и надежных наземных международных транспортных коридоров, обеспечивающих устойчивый экономический рост и потребности общества в перевозке пассажиров, движении товаров и услуг, повышение конкурентоспособности транспортной системы страны.

При этом одним из принципов обеспечения эффективности развития международных транспортных коридоров называется «повышение уровня транспортного обслуживания за счет развития транспортно-логистической и информационной инфраструктуры перевозок вдоль трассы международных транспортных коридоров», а одним из направлений повышения конкурентоспособности российских железных дорог в системе международных транспортных коридоров – «информатизация перевозок по международным транспортным коридорам, включая информационную поддержку грузоотправителей, внедрение электронного документооборота и электронной подписи».

ОАО “РЖД” активно вовлечено в развитие евроазиатских транспортных коридоров и вкладывает значительные средства в инфраструктуру с целью повышения ее пропускной способности и, соответственно, привлекательности для грузоотправителей.

В качестве одного из путей увеличения скорости международных грузоперевозок ОАО «РЖД» видит внедрение электронного обмена грузоперевозочными документами, как между администрациями взаимодействующих железных дорог, так и с таможенными органами.

На современном этапе деятельности ОАО «РЖД» и сопряженных транспортных комплексов России осуществляется широкомасштабное внедрение новых информационных технологий, обеспечивающих сбор, обработку и хранение больших объемов данных в интересах обеспечения грузовых и пассажирских перевозок. Вместе с этим работа с информацией, предназначенной для решения таких важных задач как безопасность, оперативность, рентабельность перевозок, требует использования соответствующих мер, позволяющих в свою очередь обеспечить целостность данных, авторство и неотказуемость от информации, необходимой для принятия управленческих решений. В решении перечисленных задач особое место занимает технология электронной подписи (ЭП), позволяющая наряду с обеспечением целостности информации решить задачу построения юридически значимого электронного взаимодействия и электронного документооборота.

Высокие темпы внедрения технологии ЭП для оформления грузоперевозочных документов на внутренних перевозках ОАО «РЖД» и железнодорожного транспорта сопредельных государств, таких как Белоруссия и Украина, создали предпосылки для решения задачи обеспечения юридической значимости электронного документооборота между администрациями железных дорог указанных государств.

Основой обеспечения юридической значимости является создание доверенной инфраструктуры, содержащей доверенные сервисы, которые могли бы использоваться в автоматизированных системах электронного документооборота.

Такая цель достигается путем применения сервисов доверенной третьей стороны (ДТС), которые подробно разработаны и описаны в рекомендациях как международных органов по стандартизации, так и Интернет-сообщества, и которые уже функционируют в странах Евросоюза, в Российской Федерации и во многих других странах.

Понятие «доверенной третьей стороны» и ее место в информационном взаимодействии определены, в частности, в «Соглашении о применении информационных технологий при обмене электронными документами во внешней и взаимной торговле на единой таможенной территории Таможенного союза», подписанном 21 сентября 2010 года в Москве.

При этом ДТС осуществляют взаимодействие для установления доверия при организации трансграничного электронного документооборота между субъектами электронного взаимодействия государств-Сторон, использующих разные механизмы защиты электронных документов.

В роль ДТС входит предоставление гарантий участникам взаимодействия, что сообщения и сделки своевременно и точно передаются предполагаемому получателю с обеспечением целостности, подлинности и неотказуемости от авторства, и что в случае возникновения любых споров существуют определенные методы для создания и предоставления необходимых фактов, подтверждающих совершение действий и ход событий.

В IV квартале 2012 г. – I квартале 2013 г. проводилась опытная эксплуатация технологии безбумажных перевозок порожних вагонов и грузов между БЖД и ОАО «РЖД» по электронным юридически значимым документам с применением электронной подписи.

Для обеспечения юридической значимости указанной технологии совместно с БЖД разработаны аппаратно-программные комплексы парной ДТС для проверки валидности ЭП, выработанной сопредельной стороной.

Электронный документооборот с железными дорогами Украины (Укрзализныця) осуществлялся в I квартале 2013 г. в соответствии с Временной технологией перевозки приватных порожних вагонов из Российской Федерации в Украину в прямом международном сообщении и обратно по безбумажной технологии.

Активная работа по внедрению юридически значимого электронного документооборота проводится с Казахской железной дорогой (АО «НК «КТЖ»).

Также в международном сообщении реализованы с использованием простой электронной подписи безбумажные перевозки порожних вагонов между ОАО «РЖД» и VR (Финляндия, июль 2011 г.), из Латвии (ЛДЗ) в Россию (апрель 2012 г.), из Литвы в Россию (сентябрь 2012 г.).

Упомянутые проекты по организации юридически значимого электронного документооборота между ОАО «РЖД», БЖД и АО «НК «КТЖ» призваны создать базу для внедрения такого важного и перспективного проекта как «Разработка и внедрение сквозной технологии пропуска грузопотока по международному транспортному коридору Белоруссия–Россия–Казахстан».

Разработка и внедрение инновационной технологии организации пропуска грузопотока по международному транспортному коридору является основным элементом на пути создания эффективного инструмента обеспе-

чения высококачественной услуги по перевозке грузов в межгосударственном сообщении, ускорения продвижения вагонопотоков, снижения эксплуатационных затрат. Проект закладывает основу для последующего пропуска скоростных контейнерных и контрейлерных перевозок, организации массового грузового движения в рамках транспортного коридора по согласованным сквозным ниткам графика.

Для обеспечения эффективной реализации управления транспортным коридором используется единое защищенное информационно-технологическое пространство. Примененные в проекте принципы инновационной технологии управления пропуском грузопотока могут быть адаптированы к другим международным транспортным коридорам большой протяженности с целью создания новых услуг по транзитной перевозке, исключению барьеров для беспрепятственного продвижения грузопотоков на полигоне Пространства 1520.

Dr. Matiukhin V.G.,
Scientific Director of Russian Railways
Informatics & Automatics Research & Design Institute,

TRANSBORDER DOCUMENT EXCHANGE IN JSC «RUSSIAN RAILWAYS»

In line with *The Russian Federation Strategy for the Development of Railway Transport up to 2030* setting up efficient, safe and reliable international land transport corridors that would ensure sustainable economic growth, meet the needs in the transport of passengers, goods and services and advance the competitive strength of the national transport system is one of the top priorities of Russian transport policies.

One of the fundamental principles of ensuring efficient operation of such international transport corridors is summarized as «improving the transport service by way of developing the transport-and-logistics and information infrastructure along the international transport corridors». That said, raising the level of competitiveness of the Russian railway network within the system of international transport corridors requires informatization of the process of transport through international transport corridors, including information support to shippers, introduction of electronic document circulation and digital signatures.

JSC Russian Railways is very active in developing transport corridors between Europe and Asia and invest heavily in the associated infrastructure with the view to increase the carrying capacity and, therefore, appeal for shippers.

JSC Russian Railways recognizes the fact that the speed of international traffic may be increased through the introduction of electronic exchange of shipment documents between administrations of respective railways and document exchange with customs authorities.

Presently JSC Russian Railways and associated Russian transport systems are in the process of a large-scale introduction of new information technologies enabling digital collection, processing and storage of large amounts of data to support freight and passenger traffic. At the same time, any information related to the matters of security, efficiency and profitability of traffic requires appropriate measures that ensure data integrity, copyright, and high reliability in order to facilitate the process of managerial decision-making. The above tasks will make a special use of the digital signature technology which not only solves the data

integrity problem, but also provides a technological means of communicating legally relevant documents and organizing circulation of electronic documents.

A very rapid progress of brining the digital signature technology into the operations with shipping documents for the internal traffic through the JSC Russian Railways network, as well as similar progress achieved by the rail systems of neighboring nations, such as Belarus and Ukraine, have made an important first step in building the system of electronic circulation of legally relevant documents between the administrations of the railway systems of such nations.

Legal validity of such a document exchange system must be ensured through a secure infrastructure build around trusted services to support the automated electronic document circulation system.

The above system may be built with trusted third-party services which are well developed and described in much detail by both international standardization authorities and the Internet community at large and are already in operation in the European Union, the Russian Federation and many other nations.

The definition of the «trusted third-party» and its place within the information exchange are set forth, in particular, in the *Agreement on Application of Information Technologies in the Exchange of Electronic Documents in External and Mutual Trade within the Common Customs Territory of the Customs Union* signed in Moscow on September 21, 2010.

Trusted third-parties interact to establish a trusted channel of cross-border circulation of electronic documents between the agents of electronic exchange in the CIS countries who use various protective mechanisms to secure their electronic documents.

Trusted third-parties guarantee to the parties participating in the information exchange that their communications and transactions are transmitted timely and accurately to the intended recipient while ensuring integrity, authenticity and copyright of information transmitted and that in case of any dispute there are methods to retrieve and deliver necessary evidence to support the fact of transmission and the actual course of events.

In Q4 2012 – Q1 2013 empty wagons and cargos were exchanged between the Belarusian Railway and the Russian Railways as part of the trial program for the ‘paperless’ operation using digital signatures in circulation of legal documents.

In order to ensure legal relevance of the above technology, the Russian Railways together with the Belarusian Railway developed firmware for the two trusted third-party agents to verify validity of the digital signatures produced by the other partner.

Exchange of electronic documents with the Ukrainian Railways was tested in Q1 2013 under the interim technology for the traffic of empty privately owned wagons from the Russian Federation to Ukraine and back under the 'paperless' method of operation.

We are also now actively engaged in introducing the circulation of legally relevant electronic documents into our operations with NC Kazakhstan Temir Zholy (Kazakhstan Railways).

Other international routes supporting 'paperless' traffic of empty wagons under an ordinary digital signature include JSC Russian Railways – VR (Finland, since July 2011), from Latvia (Latvijas dzelzceļš) to Russia (since April 2012) from Lithuania to Russia (since September 2012).

The above projects aimed at organizing operations supported by electronic exchange of shipping documents between JSC Russian Railways, the Belarusian Railway and NC Kazakhstan Temir Zholy are a necessary prerequisite for the implementation of such an important and ambitious project as *the Development and Introduction of End-to-end Cargo Traffic through the International Transport Corridor: Belarus–Russian–Kazakhstan.*

The development and introduction of the innovative technology of managing the freight traffic through the international transport corridor is a key element in providing a high-quality service between nations which would accelerate traffic of wagons and reduce operating costs. This project streamlines organization of future operations with high-speed container and piggyback traffic and mass traffic of cargoes through the transport corridor under an agreed schedule of operation.

Efficient management of a transport corridor requires a unified secure cyberspace. The basic principles of the innovative technology for cargo traffic control utilized in the project are adaptable to other international long mileage corridors and may provide new transit traffic services and eliminate barriers to facilitate a smooth traffic of cargoes throughout Gauge 1520.

Смелянский Р.Л.
Член-корреспондент РАН,
профессор факультета вычислительной
математики и кибернетики,
МГУ имени М.В.Ломоносова

ПРОГРАММНО-КОНФИГУРИРУЕМЫЕ СЕТИ: РЕШЕНИЕ ПРОБЛЕМЫ БЕЗОПАСНОСТИ СЕТЕЙ?

Программно-конфигурируемые сети (ПКС) представляют собой сети, в которых программно разделены управление и коммутация потоков данных, что открывает возможность программного управления пересылкой данных, которое может быть логически и/или физически отделено от физических коммутаторов и маршрутизаторов. Программно-конфигурируемые сети (ПКС) быстро совершенствуются и на данный момент используются некоторыми потребителями, в частности центрами обработки данных (ЦОД). Они обеспечивают весьма значительную экономию капиталовложений за счет замены проприетарных маршрутизаторов на общедоступные коммутаторы и контроллеры; применение абстракций из Computer Science в управлении сетями обеспечивает снижение эксплуатационных расходов с одновременным повышением технических характеристик и улучшением функциональности.

В статье рассматривается следующий вопрос, до какой степени программно-конфигурируемые сети могут решить проблемы управления сетевой безопасностью?

Что такое ПКС?

Традиционно сети определяются в терминах их физической топологии, т.е. того, как серверы, коммутаторы и маршрутизаторы соединены при помощи кабелей. Это означает, что после того, как сеть создана, новые изменения сложны и дороги. Ясно, что такой тип сетей просто несовместим с современным понятием автоматизированного центра обработки данных или облачной среды, где необходима гибкость в условиях меняющихся требований рабочей нагрузки.

В рамках подхода программно-конфигурируемых сетей, программное обеспечение может динамически конфигурировать сеть, что позволяет ей адаптироваться к меняющимся требованиям. ПКС позволяет решать несколько задач:

1. Создавать виртуальные сети, которые функционируют поверх физической сети. В multi-tenant облаке виртуальная сеть может представлять топологию сети tenant'a с его собственными IP-адресами, подсетями и даже топологией маршрутизации. С помощью ПКС виртуальные сети могут создаваться динамически и могут поддерживать мобильность виртуальных машин (VM) в рамках всего ЦОД, сохраняя абстракцию логической сети.

2. Управлять потоками трафика в сети. Некоторые виды трафика могут нуждаться в пересылке на определенные устройства (VM) для анализа безопасности или мониторинга. Может возникнуть необходимость гарантировать определенную пропускную способность или ограничить ее для некоторых загрузок. С помощью ПКС можно создавать такие политики и динамически изменять их в соответствии с рабочей нагрузкой.

3. Создавать интегрированные политики, которые соединяют физические и виртуальные сети. С помощью ПКС можно добиться, чтобы обработка трафика физической сетью и оконечными устройствами происходила схожим образом. Например, можно развернуть общие профили безопасности или обеспечить совместное использование инфраструктуры мониторинга и измерений для физических и виртуальных коммутаторов.

Таким образом, ПКС дает возможность конфигурировать конечные хосты и физические элементы сети, динамически регулировать политики управления движением трафика по сети и создавать абстракции виртуальных сетей, поддерживающие создание экземпляров VM в реальном времени и их миграцию по всему ЦОД. Программируемость ПКС включает не только конфигурирование физических элементов сети. Она значительно шире и включает программируемость конечных хостов, что делает возможной реализацию полного программного управления в центре обработки данных. Все эти функции важны для облегчения автоматизации и повышения надёжности крупных ЦОД[1].

Программно-конфигурируемые сети (ПКС):

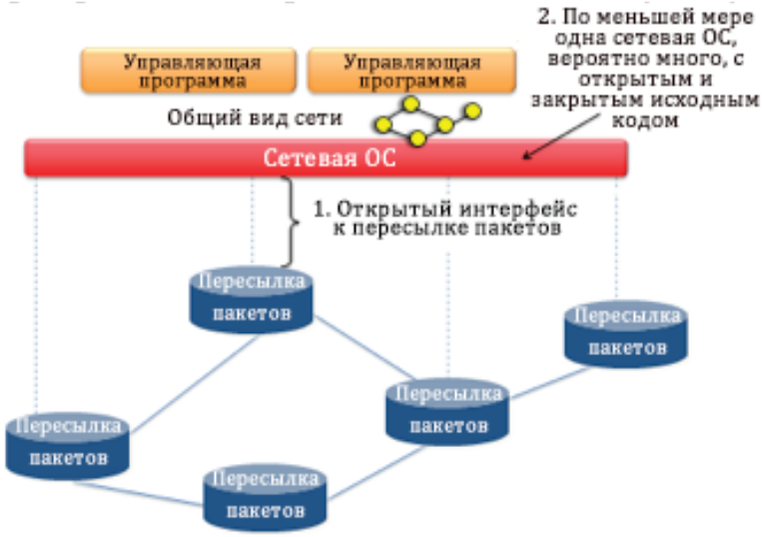


Рис. 1. Организация программно-конфигурируемой сети[289]

Безопасность в сетях традиционной архитектуры

В сети традиционной архитектуры под угрозой находятся многие элементы: инфраструктура, программное обеспечение, протоколы и т.д. В этих сетях «взлом» одного маршрутизатора может нанести серьезный ущерб сети и заказчику.

Наши дальнейшие рассуждения мы будем иллюстрировать на следующих примерах:

• Крупный транзитный поставщик услуг уровня 1 с сотнями точек присутствия (PoP) в различных странах.

• Компания, обеспечивающая некоторые услуги в филиалах крупной Международной компании в различных странах, например, услуги VPN для ее офисов в больших городах.

• Сеть крупной организации, например международного аэропорта с миллионами пассажиров, офисами авиакомпаний, представителей государственных организаций (например, службы безопасности на транспорте, пограничной службы и т.д.) и персоналом аэропорта.

В этом списке должны быть центры обработки данных. Однако, имеется огромное количество публикаций об архитектуре ЦОД и перспективах ПКС

[289] Выступление Nick McKeown, Москва, 2012.

для ЦОД. При движении вниз по списку сложность физического контроля инфраструктуры сети и степень этого контроля снижаются.

Число географически разных мест, где есть сетевое оборудование, растет в больших гетерогенных сетях. Есть заказчики, которые находятся в условиях жесткой конкуренции друг с другом. Таким образом, есть необходимость не только защищать сеть от ненадлежащего поведения приложений и заказчиков, но и защищать заказчиков друг от друга.

Термин «защита» сложен. Он означает поддержание целостности и конфиденциальности данных заказчика, предохранение от отказа сетевых сервисов (например, DDoDs) и т.д. При современном развитии сетевых технологий, огромном росте пропускной способности Интернета и переходе от стационарных клиентских устройств к мобильным сетям (имеется уже 1 миллиард подключенных смартфонов в начале 2013 г. и только около 200 тысяч стационарных устройств), эффективность существующих решений управления доступом снижается. Для каждой новой версии протокола Ethernet нужны все более дорогие устройства для сетей одного и того же масштаба, что пять или десять лет назад. В терминах мобильности клиентских устройств, сетевые конфигурации быстро меняются, и изменения информации о топологии сети не могут использоваться непосредственно для управления доступом. Таким образом, проблема управления доступом к сети на основе информации об ожидаемом поведении (потоках) сетевых приложений становится все более важной.

Инфраструктура

Одна из основных угроз в области инфраструктуры — физический доступ к сетевым устройствам. В большом аэропорту невозможно гарантировать физическую недоступность сетевых устройств. Как только злоумышленник получает доступ к устройству, он может полностью или частично изменить его содержимое. Злоумышленник также может получить доступ к сетевым кабелям. Это еще один пример угрозы в этой области. Такой доступ предотвратить невозможно. Например, если поставщику услуг необходимо заменить какое-то сетевое устройство в его сети, то никто не может гарантировать, что оборудование по пути с завода на склад поставщика не будет изменено.

В сети ПКС ситуация совершенно другая. Все интеллектуальные функции удалены с маршрутизаторов и коммутаторов и помещены на контроллеры сети ПКС (см. рис. 1). Сервер с контроллером можно легко перенести в надежно защищенное помещение. Программируемые контроллеры мо-

гут поддерживать набор так называемых приложений (с-приложение или управляющая программа на рис. 1), которые обеспечивают традиционные сетевые сервисы, такие как маршрутизация, защита от перегрузок, управление QoS и т.д., а также новые сервисы, такие как виртуализация, фильтрация (как обычные брандмауэры), обнаружение вредоносных программ и т.д. В данном контексте сервисы виртуализации означают разделение.

Программное обеспечение

Программное обеспечение в сети ПКС сконцентрировано в контроллерах. Таким образом, один из ключевых вопросов — где следует разместить контроллер ПКС [2]. Сегодня уже ясно, что должна быть иерархия контроллеров с различными наборами приложений.

В этой иерархии должно быть не менее двух уровней. На верхнем уровне должен находиться контроллер управления инфраструктурой. Контроллеры этого уровня выдают разрешения на предоставление ресурсов по запросу пользователя. Они играют роль управления ресурсами инфраструктуры. Например, в аэропорту новая авиакомпания или новая организация обратится с запросом на выделение ресурсов. В этом запросе она указывает необходимый тип ресурсов, количество каждого вида ресурсов и требуемое качество обслуживания. Контроллеры на следующем более низком уровне отображают виртуальные ресурсы на физические. Они выдают набор правил для соответствующих коммутаторов.

Каждый контроллер должен реализовывать следующие функции:

- контроллеры на одном и том же уровне должны иметь один и тот же набор с-приложений;
- с-приложения должны быть пригодны для многократного (reusable) использования контроллерами, размещаемыми поблизости один от другого;
- различные экземпляры контроллера должны быть способны совместно использовать один экземпляр n-приложения;
- контроллер должен быть доверенной (trusted) средой;
- контроллер должен быть масштабируемым; это означает, что при возрастании рабочей нагрузки выше определенного уровня, контроллер должен быть способен получить дополнительную вычислительную мощность, например путем разделения своей работы с другим экземпляром контроллера, размещенным на другом физическом ресурсе;

• если один из экземпляров контроллера неожиданно прекратил работу, другие контроллеры, размещенные поблизости, должны взять на себя ту часть сетевых коммутаторов, которая управлялась отключившимся контроллером.

Безопасность с-приложения представляет собой другую проблему. Здесь мы сталкиваемся с той проблемой, какая возникает у тех, кто работает с приложениями для iPhone, Android и т.д. Хорошим решением этой проблемы могло бы быть описание поведения с-приложения [3]. Кажется, этот подход будет более эффективным и менее ресурсоемким, чем, например, формальная верификация и проверка на моделях (model checking) [4].

Мониторинг — другая ключевая функция для безопасности ПКС сетей. Должно вестись несколько видов мониторинга. Мониторинг поведения с-приложений — одна из этих задач. Другая — мониторинг и проверка пакетов. Это важно как для сбора образцов потоков данных, так и для того, чтобы убедиться в том, что виртуализация разделила потоки данных надлежащим образом, например, потоки данных конкурентов никогда не пересекаются. Мониторинг является важной функцией системы реагирования. При проникновении злоумышленника система должна реагировать должным образом для восстановления работы контроллера. Не имеет значения, в какой форме выступает злоумышленник — как несанкционированное программное обеспечение, неправильно ведущее себя с-приложение или что-то другое.

Протоколы

Рассмотрение безопасности протоколов мы разделим на следующие части:

1. безопасность протокола контроллер-коммутатор;
2. безопасность протоколов с-приложений;
3. безопасность протоколов контроллер-контроллер.

Безопасность протоколов контроллер-коммутатор. В типичном сегменте сети ПКС между коммутатором и контроллером используется безопасное соединение SSL. SSL обеспечивает базовый уровень безопасности, но в реальных условиях ПКС сети его может быть недостаточно (например, развитые криптографические протоколы: Internet Key Exchange, IPsec, Kerberos и т.д.). Эти методы шифрования могут быть достаточны для ЦОД, но вряд ли подойдут для сетей WAN и даже для автономных систем. Здесь возникают все проблемы, связанные с управлением ключами, с возрастанием расходов и задержками шифрования [5,6].

Безопасность протоколов с-приложений. Одна из проблем здесь заключается в том, достаточно ли существующих решений и будут ли другими решения для с-приложений ПКС? Например, как безопасно загрузить ключи в устройство. Другим примером может быть вопрос о том, где надлежащее место для с-приложения для анализа трафика на контроллере. Но приложения контроллера концентрируются только на анализе заголовков сетевых пакетов. Вот почему не рекомендуется помещать DPI-функцию на контроллер, поскольку она требует передачи тела пакета на контроллер. Тело пакета никогда не должно обрабатываться на стороне контроллера.

Безопасность протоколов контроллер-контроллер. Скорее всего, в ближайшем будущем ПКС-контроллеры будут работать в локальной распределенной компьютерной среде. В таком случае можно использовать протоколы SSL/TLS. Основным компонентом распределенного контроллера является протокол взаимодействия нескольких контроллеров в локальной среде. Предполагается, что такой протокол может работать двумя способами: “out-band” и ”in-band”. При “out-band” создается отдельная сеть управления из контроллеров, и нет необходимости защиты сети. При ”in-band” необходимо создать защищенный канал данных между контроллерами. В случае WAN или MAN для связи между контроллерами будет два случая. Либо этот протокол будет работать в плоскости данных, тогда будут необходимы изощренные методы обеспечения безопасности. Если будет выделенная плоскость управления, недоступная из плоскости данных, то можно будет использовать более простые методы. Мы должны постоянно помнить, что простота - это сила.

Рассматривая безопасность ПКС в случае WAN, мы должны понимать, что контроллер будет чрезвычайно привлекательной мишенью для злоумышленника. И здесь мы сталкиваемся с проблемой идентификации (fingerprinting). Другими словами: как идентифицировать, управляется ли сегмент сети контроллером ПКС или представляет собой обычную для традиционных сетей смесь плоскости данных и плоскости управления? В этом случае наиболее вероятный подход — использовать отклонения таймаута при установлении соединения с конкретным сегментом.

Остается одна область, которая здесь не была рассмотрена — безопасность протоколов сетевых приложений. В этой области у нас все еще есть вопросы без ответов: должно ли сетевое приложение поддерживать какую-либо связь с с-приложением?

Исходя из принципов сетевой безопасности ответ должен быть Нет. Однако практика показывает, что по многим причинам было бы полезно,

чтобы между ними поддерживалась связь. Один из примеров — управление качеством обслуживания.

Заключение

Программно-конфигурируемые сети (ПКС) быстро совершенствуются и на данный момент используются, в частности, центрами обработки данных. Они обеспечивают весьма значительную экономию капиталовложений за счет замены проприетарных маршрутизаторов на общедоступные коммутаторы и контроллеры; применение абстракций из Computer Science в управлении сетями обеспечивает снижение эксплуатационных расходов с одновременным повышением технических характеристик и улучшением функциональности.

ПКС подход имеет много преимуществ в области безопасности, особенно в части физической безопасности сетевого оборудования. Разделение плоскости данных и плоскости управления дает дополнительные преимущества. Однако необходимо исследовать еще очень многое, особенно в области программного обеспечения ПКС. Примером одной из таких областей является протокол связи коммутатор-контроллер и контроллер-контроллер.

Одной из основных возможностей ПКС подхода является удобство и гибкость конфигурирования политик коммутации (forwarding policy). С помощью протокола OpenFlow можно не только конфигурировать пересылку конкретных типов трафика через определенные точки сети, но также проверять, все ли сетевые пакеты проходят через эти конкретные точки. Это дает огромные возможности для сетевой безопасности, но все еще требует исследований.

Литература

1. http://blogs.technet.com/b/windowsserver/archive/2012/08/22/software-efined-networking-enabled-in-windows-server-2012-and-system-center-2012-sp1-virtual-machine-manager.aspx

2. Heller, R. Sherwood, and N. McKeown, "The controller placement problem," in Proceedings of the first workshop on Hot topics in software defined networks, ser. HotSDN '12. ACM, 2012, pp. 7–12.

3. R.L.Smeliansky, D.Gamaynov "The model of network applications behavior.", Moscow, *Programmirovanie*, 2007, № 4, pp.1-12 (P*rogramming and Computer Software*, ISSN 0361-7688, 2007, Vol. 33, No. 6, pp. 308–316. ©*Pleiades Publishing, Inc*., 2007.)

4. Edmund M. Clarke, Jr., Orna Grumberg and Doron A. Peled, Model Checking, MIT Press, 1999, ISBN 0-262-03270-8.

5. M.Lepinski (Ed.) "BGPSEC Protocol Specification," Internet Engineering Task Force, Feb. 2013. [Online]. Available: http://www.ietf.org/id/draft-ietf-sidr-bgpsec-protocol-07.txt

6. Domain Name System Security Extensions. RFC 2535

R.L.Smelyanskiy
Corresponding member,
Russian Academy of Sciences Professor,
Faculty of Computational Mathematics and Cybernetics,
MSU, Russia

SDN: IS IT A SOLUTION FOR NETWORK SECURITY?

Software **D**efined **N**etworking, **SDN**, is the programmable separation of control and forward elements of networking that enables software control of network forwarding that can be logially and/or physically separated from physical switches and routers. Software Defined Networking (SDN) is developed rapidly and used now by early adopters such as data centers. It offers immediate capital cost savings by replacing proprietary routers with commodity switches and controllers; using of computer science abstractions in network management offers operational cost savings, with performance and functionality improvements as well.

The following great question is considered in this paper: to what extend SDN–based networks can address network security management problems?

What is SDN?

Traditionally, networks are defined by their physical topology i.e. how servers, switches and routers are cabled together. That means that once you have built out your network, changes were costly and complex. Certainly, this type of networking is simply not compatible with the notion of a lights-out datacenter or a cloud environment that need flexibility to support varying workload demands.

Under Software Defined Networking approach software can dynamically configure the network, allowing it to adapt to changing needs. An SDN solution can accomplish several tasks:

1. Create virtual networks that run on the top of the physical network. In a multi-tenant cloud virtual network might represent a tenant's network topology complete with the tenant's own IP addresses, subnets, and even routing topology. Through SDN virtual networks can be created dynamically, and can support VM mobility throughout the datacenter while preserving the logical network abstraction.

2. Control traffic flow within network. Some classes of traffic may need forwarding to a particular appliance (or VM) for security analysis or monitoring.

You may need to create bandwidth guarantees or enforce bandwidth caps on particular workloads. Through SDN, you can create these policies and dynamically change them according to the needs of your workloads.

3. Create integrated policies that span the physical and virtual networks. Through SDN, you can ensure that your physical network and endpoints handle traffic similarly. For example, you may want to deploy common security profiles or you may want to share monitoring and metering infrastructure across both physical and virtual switches.

In summary, SDN is about being able to configure end hosts and physical network elements, dynamically adjust policies for how traffic flows through the network, and create virtual network abstractions that support real-time VM instantiation and migration throughout the datacenter. SDN programmability include not only configuration of physical network elements. It is much broader and includes programmability of end hosts, enabling end-to-end software control in the datacenter. All these features are important to facilitate automation and reliability in large-scale datacenters [1].

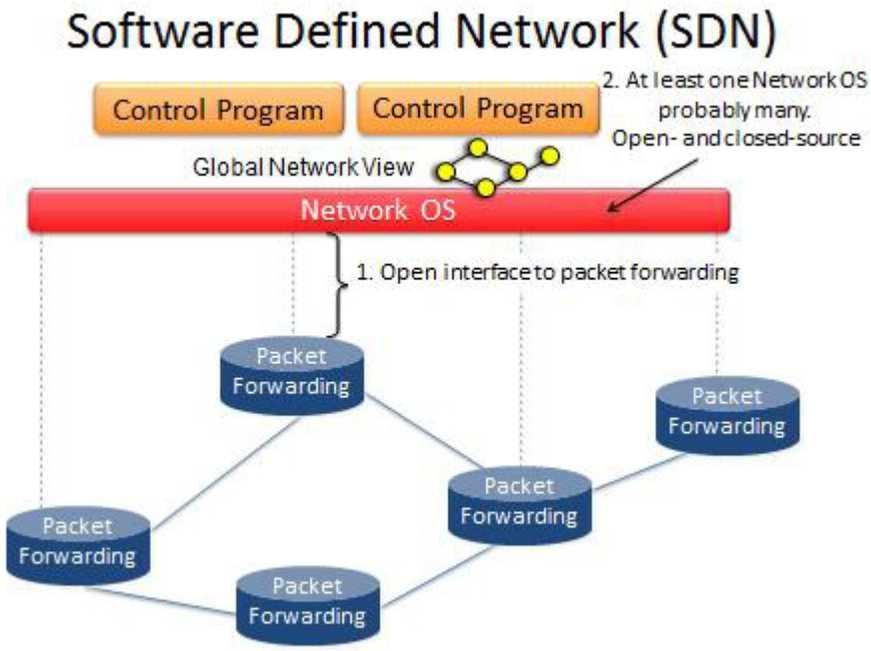


Figure1. Software Defined Network organization[290]

[290] Nick McKeown Moscow talk 2012.

Security in traditional architecture networks

In network with traditional architecture there are many areas under threats: infrastructure, software, protocols etc. In those networks the compromising of one router can cause a serious damage to the network and its customers.

We will conduct our further consideration with next case studies:

- Large Transit Service Provider kind of Tier-1 with hundreds Points of Presence (PoP) in different countries.

- The company which provides some services to the branches of big International Company (Inc.) in different countries, e.g. VPN Services for Inc. offices in big cities.

- Network of Large Organization like International Airport where there are millions of passengers, airlines offices, state organization representatives (e.g. TSA, Immigration Service, etc.), and airport staff.

There should be Data Centers in this list. However, there are a lot of publications about DC architecture and SDN perspectives for DC. Along down the list of complexities of physical control over network infrastructure and this control itself decrease.

The number of geographically distributed locations with network equipment is growing in a large heterogeneous network. There are customers which are strongly engaged in competition with each other. So, there is a need not just to protect network from misbehavior of application and customers, but to protect customers from each other.

The term “protecting” is complex. It means integrity and confidentiality of customer’s data, protecting from the fall down of network services (like DDoDs) etc. Nowadays under evolved networking technologies, enormous growth of Internet throughput and a shift from fixed client devices towards mobile networking (we have over 1 billion connected smartphones already in early 2013, and only about 200 million fixed devices) efficiency of existing access control solutions reduces. More expensive devices are required for every new version of Ethernet protocol providing the same level of network granularity as five or ten years ago. In terms of client devices mobility, network configurations are changing rapidly and the information on network topology changes could not be used directly for access control. So the problem of network access control based on the information on the expected behavior (flows) of network applications is becoming more and more important.

Infrastructure

One of the main threats in this area is a physical access to the network devices. In a big airport it`s impossible to guaranty physical inaccessibility to the network devices. Once trespasser gain the physical access to the device, he/she can modify, replace internals of that device. A trespasser can gain access to the network cabling as well. This is another example of the threat in this area. It is impossible prevent such an access. For example if the Provider needs to exchange some network equipment in its network, nobody can guaranty that the equipment on its way from a factory to the Provider location would not be modified.

There is absolutely different situation in SDN network. All intelligence got away from the routers and switches and places into SDN network controllers (see figure 1). The server with controller easily could move into well protect environment. Programmable controllers can support the set of so called applications (c-application or control program on figure 1) which will supply as ordinary, traditional network services like routing , congestion avoidance, QoS management etc. as a new one such as virtualization, filtering (as ordinary firewalls), malware detection etc. In this context virtualization services mean separation.

Software

Software in SDN network is concentrated in controllers. So, one of the key question is where SDN controller should be placed [2]. As it is seen today there is a hierarchy of controllers with different set of applications.

This hierarchy should have at least two levels. On the top level should be a controller for infrastructure management. Controllers on this level issue the approval for resources allocation under user request. They play a role of infrastructure resources managers. For example at the airport new airline or new company will issue the request for resources. In this request it describes what kind of recourses are needed, amounts for each kind of recourses and required QoS. The mapping of virtual recourses on physical ones is implemented by the controllers on the next low level. They issue the set of proper rules for the corresponding switches.

Each controller should implement the following functions:

- controllers on the same level should have the same set of c-applications;
- c-applications should be reusable by different controllers placed near-by each other;
- different controller instances should be able to share the same instance of an n-application;

• controller should be trusted environment;

• controller should be scalable; it means that if workload is growing beyond the current computational power of controller then it should be able to get more computational power, for example by splitting its activity with another controller instance, placed on another physical resource;

• if some controller instance is shut down, then some other controllers placed nearby should be able to catch up those part of network switches that were managed by controller instances which are shut down.

A secure n-application is another problem. Here we faced with the same problem like people had with applications for iPhone, Android etc. A good solution for such problem could be the description of c-application behavior [3]. It seems this approach will be more effective, not resource consuming like formal verification e.g. and Model checking [4].

Monitoring is another crucial function for SDN network security. There should be different kind of monitoring activities. c-application behavior monitoring is one of the activities. Another one is packet monitoring and inspection. It is important as for sampling of a data flows as for get sure that virtualizing has separated data flows properly, e.g. the data flows of competitors never crossing. Monitoring is important function for reaction system. Once a trespasser is detected such system should react properly up to restore the controller operation. It doesn't matter of what form a trespasser has, e.g. unauthorized software, misbehavior n-application etc.

Protocols

Talking about protocol security we will split the consideration on the following parts:

• Switch-controller protocol security;

• c-Application Protocol security;

• Controller-controller protocol security.

Switch - controller security. In typical SDN network segment between switch and controller SSL secure connection is used. SSL provides the basic security level and that in real-network SDN deployment may not be enough (for example, advanced cryptographic protocols: Internet Key Exchange, IPsec, Kerberos and etc.). These inscription technics could be enough for Data Centers but hardly would be appropriate for WAN networks or even for Autonomous Systems. Here all problems related to key management, appeare with increase cost and delays for encryption [5,6].

c-Application protocol security. One of the problem is whether the existing solutions enough and are there any different for SDN n-applications? One of such point is how key could be bootstrapped into a device in a secure way? Another example could be such as a native place for traffic analysis is an n-application over controller. But controller applications focus only on network packet header analysis. That's why it is not recommended to put deep-packet inspection functions on controller, because it requires forwarding packet payload to controller. A payload must never be executed on a controller side.

Controller - controller protocol security. Most likely that in nearest future SDN controllers will run in a local distributed computer environment. In such cases SSL/TLS protocols could be used. The major component of distributed controller is protocol among several controllers in a local environment. Supposedly, such protocol can operate in two ways: out-band, and in-band. In case of out-band a separate control network among controllers is building and there is no necessity to network protection. In case of in-band it is important to provide secure channel to forward data among controllers. In the case of WAN or MAN for controllers communications will have two cases. Either the protocol run in a data plane it will require new sophisticated security technics. If there will be separated control plane which is inaccessible through data plane much easier security technics would be used. And every time we have to remember that the simplicity is a power.

Considering SDN security in the case of WAN we have to understand that a controller would be extremely desirable target for trespasser. In this way we come to the fingerprinting problem. Another word: how to distinguish is the network segments controlled by SDN controller or have traditional network communication mixture of data plane and control plane? In that case the most probable approach is to use timeout deviations while the connection process to concrete segment.

There is one area was not considered so far here is network Application Protocol security. In this area we still have unanswered question: Does network application should have any communication with c-application?

From informational security principals the answer should be No. However the practice show that for the many reason it could be useful to let them communicate. On of such kind of example could be the quality of Service management.

Conclusion

Software Defined Networking (SDN) has been developed rapidly and is now used by early adopters such as data centres. It offers immediate capital cost savings by replacing proprietary routers with commodity switches and controllers;

computer science abstractions in network management offer operational cost savings, with performance and functionality improvements too.

SDN network has a lot of advantages for network security especially in physical security of network equipment. Splitting data plane and control plane bring a lot of new ones. However there is a lot researching has to be done especially in SDN software area. The example of one of such area could be security protocol in switch-controller and controller-to-controller communication.

The major opportunity of SDN approach is convenient and flexible configuration of packet forwarding policy. Using functionality of OpenFlow protocol, we could not only configure forwarding of concrete traffic types to go through special network points, but also verify that all the network packets come thought these specific points. This is feature sounds like a lot of opportunities for network security but still required researching.

Bibliography

1. http://blogs.technet.com/b/windowsserver/archive/2012/08/22/software-efined-networking-enabled-in-windows-server-2012-and-system-center-2012-sp1-virtual-machine-manager.aspx

2. Heller, R. Sherwood, and N. McKeown, "The controller placement problem," in Proceedings of the first workshop on Hot topics in software defined networks, ser. HotSDN '12. ACM, 2012, pp. 7–12.

3. R.L.Smeliansky, D.Gamaynov "The model of network applications behavior.", Moscow, *Programmirovanie*, 2007, № 4, pp.1-12 (P*rogramming and Computer Software*, ISSN 0361-7688, 2007, Vol. 33, No. 6, pp. 308–316. ©*Pleiades Publishing, Inc*., 2007.)

4. Edmund M. Clarke, Jr., Orna Grumberg and Doron A. Peled, Model Checking, MIT Press, 1999, ISBN 0-262-03270-8.

5. M.Lepinski (Ed.) "BGPSEC Protocol Specification," Internet Engineering Task Force, Feb. 2013. [Online]. Available: http://www.ietf.org/id/draft-ietf-sidr-bgpsec-protocol-07.txt

6. Domain Name System Security Extensions. RFC 2535

Пилюгин П.Л., Сальников А.А.
Институт проблем информационной безопасности
МГУ имени М.В.Ломоносова

ПОНЯТИЕ «ДОВЕРИЕ» В МОДЕЛИРОВАНИИ КИБЕРКОНФЛИКТОВ

При обсуждении вопросов взаимодействия в киберпространстве (Интернет, социальные сети, финансовые транзакции и т.д.) вместо понятий «надежность», «безопасность», «защищенность» (и их характеристик, которые можно измерять) все чаще используют понятие – «доверие». Более того, ряд авторов полагают, что понятие «доверие» может полностью заменить традиционные характеристики безопасности.

Это, прежде всего, связано с экономическими вопросами – продажи в киберпространстве оборудования, программ, сервисов, информации и других товаров и услуг, где покупателю зачастую недоступны объективные характеристики приобретаемых товаров и услуг.

Излишнее доверие при этом может быть небезопасным. Например, как показали исследователи из университетов Пенсильвании и Дьюка, а также лаборатории Intel Labs®, две трети приложений под операционную систему Android® отслеживают набираемые номера, собирают сведения о географическом позиционировании аппарата (телефона, компьютера и т.д.) и осуществляют другую «подозрительную» активность по отношению к персональным сведениям.

В связи с этим представляется полезным более точно охарактеризовать понятие «доверие» и определить его место в вопросах возникновения, развития и устранения киберконфликтов.

Киберконфликт с позиций «Единой теории конфликтов»

Единая теория конфликтов (ЕТК) [3] рассматривает конфликт, как диалектическое противоречие, приводящее систему в движение. Результат конфликта – синергизм или антагонизм.

При синергизме все взаимодействующие системы связаны друг с другом прямо пропорциональными связями. Поэтому синергизм развивается как симметричное усиление (или ослабление) системами активности друг друга. Синергизм – это сосуществование (сотрудничество, объединение в одну систему) систем или элементов системы, когда их свойства улучшаются или ухудшаются одновременно.

Антагонизм, который часто отождествляют с конфликтом, – это такое сосуществование элементов системы, когда изменение свойств элементов системы разнонаправлено. Можно считать, что антагонизм объединяет в одну общую систему элементы, разделяя при этом их на два полюса (коалиции) таким образом, что, элементы каждой коалиции связаны друг с другом прямо пропорциональными, а с членами противоположной коалиции обратно пропорциональными связями.

Взаимодействия (в том числе, конфликты) в киберпространстве обладают своими особенностями. Часто события обычно называемые киберконфликтами по сути являются уже кибервойнами. Как пример, можно вспомнить недавнюю кибератаку (или киберконфликт) между активистами двух групп: команды из Лондона/Женевы Spamhaus и нидерландской команды Cyberbunker. По сути это конфликт, который является антогонизмом экономических интересов спамеров и антиспамеров. Такого разрешения конфликта можно было бы избежать, если более действенно бороться со спамом на законодательном уровне или наоборот – запретить все преграды по распространению любой информации.

Участниками взаимодействий (в том числе и конфликтов) в киберпространстве являются пользователи (возможно объединенные коммерческими, общественными или государственными организациями), провайдеры (услуг, сервисов, связи, контента и т.д.), а также программы и оборудование, а через них и их производители.

В предлагаемой модели участники, предметы и причины конфликта соединены положительными (сотрудничество, согласие) или отрицательными связями. Анализ модели позволяет выявлять конфликтные ситуации и разрешать их путем изменения отрицательных связей на положительные и наоборот.

Роль доверия в процессе развития киберконфликтов

С учетом понимания того, что СИНЕРГИЗМ это сотрудничество, а АНТАГОНИЗМ это конфронтация, необходимым условием для развития конфликта является ДОВЕРИЕ без которого невозможно сотрудничество и соответственно НЕДОВЕРИЕ при установлении антагонистических отношений. Предложенная ЕТК схема развития конфликта условно приведена на рисунке.

В соответствии с ЕКТ, как синергизм, так и антагонизм могут быть приемлемыми результатами разрешения конфликта. И если развитие доверия для перехода к сотрудничеству, очевидна, то менее очевидна задача уменьшения излишнего доверия для сглаживания негативных эффектов антогонизма.

В первом случае примером могут служить программы и оборудование, хорошо зарекомендовавшие себя на практике и достаточно открытые благодаря политике производителей.

Примером второго подхода является излишняя (необоснованная) доверчивость пользователей социальных сетей и других Интернет-сервисов, которая приводит к утечке персональных данных, а также к финансовым потерям.

В обоих случаях возникает задача введения меры и способов измерения доверия.

Модели (метрики) доверия

В последнее время используются различные механизмы измерения доверия (репутации), что особенно актуально в виртуальных сообществах и системах электронной торговли [5]. Проблемам доверия и репутации в онлайновых системах посвящено большое количество исследований [6], в том числе по экономике (формирование репутации и социальное обучение), компьютерным наукам (вычислительные модели доверия и репутации, вопросы масштабируемости, распределенности и безопасности вычислений), социологии и психологии (рациональность, важность эмоциональных и когнитивных факторов), науке о методах управления (влияние репутации/доверия в маркетинге, создании бренда и т.п.), а также политологии (влияние репутации на общественное мнение).

Простое суммирование или среднее значение оценок

При этом подходе, значение репутации является суммой положительных и отрицательных откликов. Пример использования – eBay. Такой метод подсчета примитивен и значение репутации получается грубым. Преимуществами данного метода являются прозрачность и понятность для пользователя. Более сложные схемы используются в Epinions и Amazon. В этих системах производится суммирование взвешенных оценок (веса определяются в зависимости от репутации, времени оценки, расстояния и т.п.)

Модели агрегирования оценок доверия

Использование понятий доверия и репутации, ориентированных на электронную коммерцию и взаимодействие в социальных сетях, применяет различный математический аппарат для агрегирования оценок:

- Abdul-Rahman и Hailes – теория графов [7];
- Advogato Trust Metric – потоки в сетях [8];
- Байесов подход (модель на основе бета-функции распределения [9] и модель субъективной логики [10]);
- модель решетки [12].

Из приведенного перечня моделей отметим, что модель Abdul-Rahman и Hailes, а также модель решетки ориентированы не на количественные, а на качественные показатели доверия (что более естественно и удобно для оценок).

Модель аналитических зависимостей

Более общую формализацию доверия дает в своей работе [13] С.Марш. Он предлагает вводить множество переменных и способ их объединения для

получения одного значения доверия в диапазоне [-1; 1]. Так как эта модель будет использоваться далее, приведем используемые в ней обозначения и соотношения для базового, общего и ситуационного доверия, в зависимости от знаний (опыта), важности и полезности в данной ситуации:

Наименование	Обозначение	Область значение
Ситуации	α β γ δ ε	
Участники (акторы, агенты)	a, b, c	
Знания (например x знает y)	Kx(y)	0, 1
Важность (т. е. важность для x ситуации α)	Ix(α)	[0,+1]
Полезность (т. е. полезность для x ситуации α)	Ux(α)	[-1,+1]
Базовое доверие (т.е. доверчивость x)	Tx	[-1,+1)
Общее доверие (x доверяет y)	Tx(y)	[-1,+1)
Ситуационное доверие	Tx(y,α)	[-1,+1)
Порог сотрудничества (в ситуации α)	CTx(α)	
Ожидаемый риск	PRx(α)	[0,1]
Ожидаемая компетентность	PCx(y,α)	[0,1]
Ожидаемая полезность	PUx(y,α)	[0,1]

Эти характеристики связаны следующими соотношениями:

$$T_x(y,\alpha)=U_x(\alpha)\cdot I_x(\alpha)\cdot T_x(y)^*$$

или в более сложной зависимости:

$$T_x(y,\alpha)=(U_x(\alpha)+T_x(y)^*)\cdot I_x(\alpha)\cdot T_x(y)^{*\,x},$$

где:

$T_x(y)^*$ – обозначает оценку доверия x по отношению к y (среднее значение доверия во всех возможных ситуациях; другими словами репутация);

$T_x(y)^{*\,x}$ – субъективная оценка доверия x по отношению к y (средняя оценка доверия, но с учетом знаний x о y).

В модели С.Марша предполагается, что эти значения могут меняться во времени. Это позволяет рассматривать «глубину» памяти, однако приводит к более сложным зависимостям, которые здесь рассматриваться не будут.

Значения доверия используются, чтобы помочь агенту принять реше-

ние о взаимодействии с другим агентом на основе некоторого порога. Сотрудничество x и y в ситуации α возможно, если ситуационное доверие выше некоторого порога:

$T_x(y,\alpha)$ > Cooperation_Thresholdx(α) => возможно сотрудничество, где порог кооперации Cooperation_Thresholdx(α) определяется, например, исходя из ожидаемого риска и ожидаемой компетенции контрагента и важности ситуации:

$$Cooperation\_Threshold_x(\alpha) = (PR_x(\alpha) / PC_x(y,\alpha))\cdot I_x(\alpha)$$

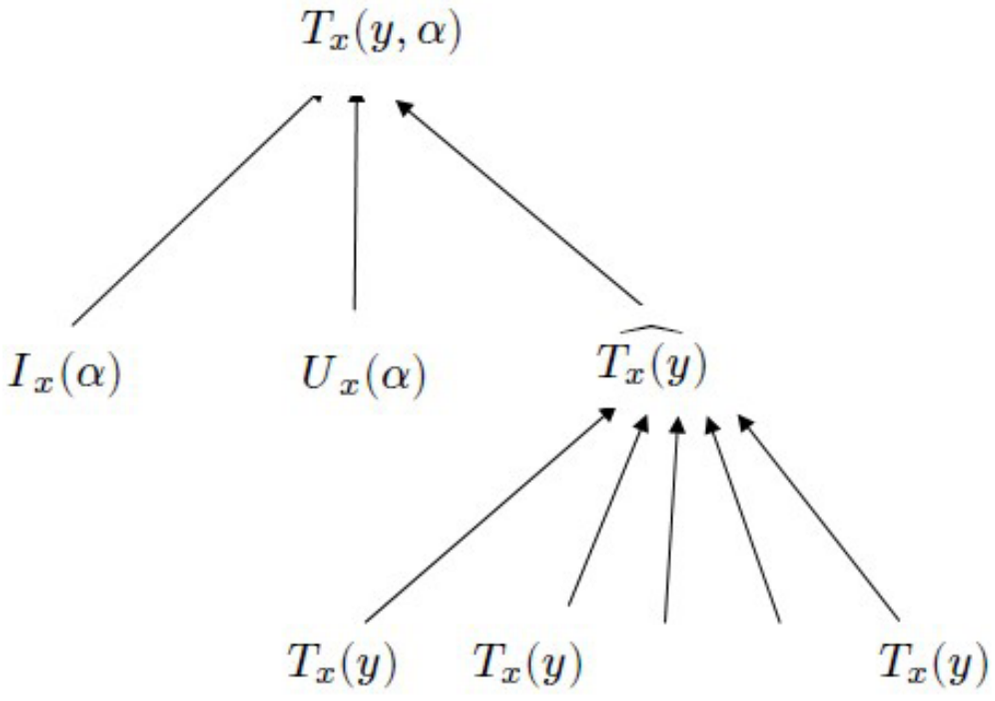
или более точно:

$$Cooperation\_Thresholdx(\alpha) = (PR_x(\alpha) / (PC_x(y,\alpha) + T_x(y)^*))\cdot I_x(\alpha)$$

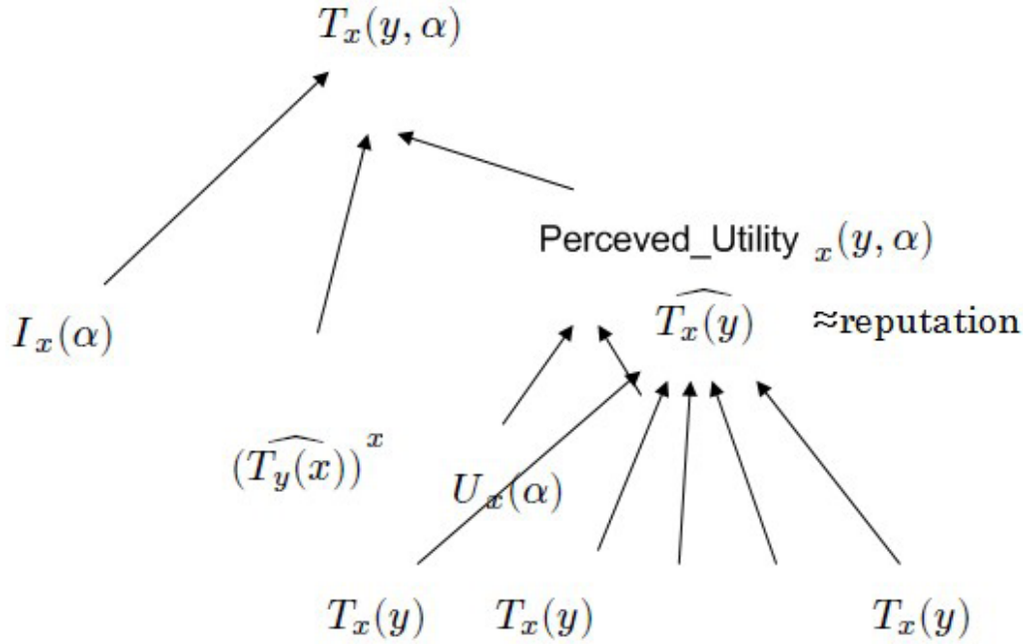
Построение модели измерения в качественных шкалах

На примере приведенной выше аналитической модели покажем возможность построения модели с измерением основных характеристик в качественных шкалах. При этом результат измерения доверия будет находиться уже не в интервале [-1; 1], а принадлежать некой качественной шкале (например: «очень плохо», «плохо», «удовлетворительно», «хорошо», «отлично»). В качестве такой шкала будем в дальнейшем использовать шкалу рангов с n градациями.

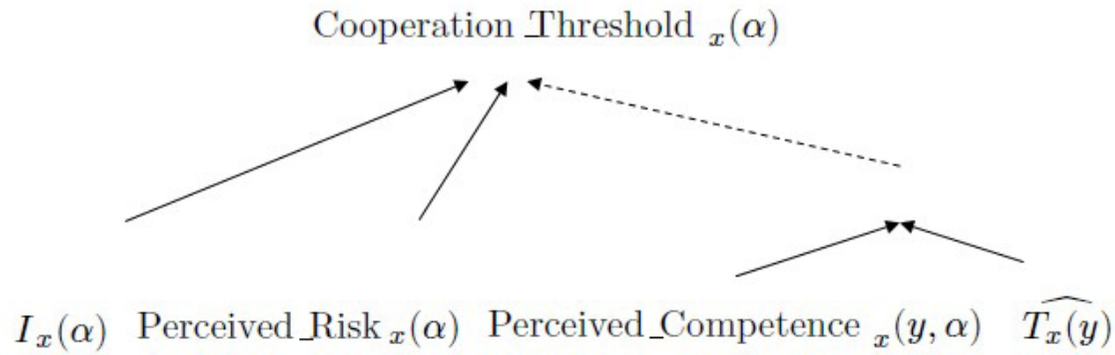
Предполагая, что все приведенные выше обозначения измерены в одинаковых качественных шкалах (причем доверие и недоверие будут рассматриваться отдельно), представим приведенные выше аналитические зависимости виде:



или, соответственно:



и для порога кооперации:



Для таких иерархических структур ранее рассматривались (см., например, [14]) различные методы агрегирования и преобразования шкал: лексикографическое упорядочение (построение отношения порядка на декартовом произведении множеств), метод сумм рангов и т.д. Поскольку в нашем случае иерархические структуры построены из аналитических выражений, то целесообразно использовать свертки шкал соответствующие арифметическим действиям, с сохранением размерности шкал.

В общем случае задача построения таких сверток представляет задачу построения линейного порядка на декартовом произведении линейно упорядоченных множеств одинаковой размерности n и объединении элементов этого произведения в n классов эквивалентности. На таком декартовом произведении индуцируется отношение частичного порядка:

$$(i,j) \geq (k,l) \iff i \geq k \ \& \ j \geq l,$$

где *i,j,k,l* индексы линейно-упорядоченных множеств и их декартова произведения.

Используя подход, основанный на упорядочении суммы и произведения рангов, можно получить мультипликативную и аддитивную свертки, удовлетворяющие индуцированному отношению частичного порядка.

Ниже для ранговых шкал с 5-ю градациями приведены примеры сверток – (x) - мультипликативной и (+) - аддитивной:

x	1	2	3	4	5
1	1	1	1	1	1
2	1	2	2	2	2
3	1	2	3	3	3

+	1	2	3	4	5
1	1	2	3	4	5
2	2	2	3	4	5
3	3	3	3	4	5

Для операций деления и вычитания построение сверток менее очевидно. В этом случае для одного из линейно упорядоченных множеств отношения порядка изменяется на противоположное, что соответственно модифицирует отношение частичной упорядоченности на декартовом произведении множеств:

$$(i,j) \geq (k,l) \iff i \leq k \ \& \ j \geq l,$$

где *i,j,k,l* индексы линейно-упорядоченных множеств и их декартова произведения.

Ниже приведены примеры сверток ранговых шкал с 5-ю градациями соответственно для операций деления (/) и вычитания (-), основанные на упорядочении частного и разности рангов и удовлетворяющие новому отношению порядка на декартовом произведении множеств:

/	1	2	3	4	5
1	3	1	1	1	1
2	5	3	2	2	2
3	5	4	3	2	2

-	1	2	3	4	5
1	3	2	1	1	1
2	4	3	2	1	1
3	5	4	3	2	1

Полученные способы свертки шкал могут быть обобщены для шкал с произвольным количеством градаций, однако приведенное число градаций удобно для практических вычислений, что будет использовано ниже.

Проведем сравнение результатов анализа модифицированной формулы для Cooperation_Thresholdx(α), приведенных в описании модели С.Марша [13], с данными получающимися при переходе к качественным шкалам при $I_x(\alpha)=1$.

Таблица модели $Cooperation\_Threshold_x(\alpha)$

		-1	Ожидаемая компетенция $PC_x(y,\alpha) + T_x(y)^*$				
		-0,5	0	+0,5	+1	+2	
Рискл. $PR_x(\alpha)$	0	**0**	**0**	**∞**	**0**	**0**	**0**
	+0,5	**-0,5**	**-1**	**∞**	**+1**	**+0,5**	**+0,25**
	1	**-1**	**2**	**∞**	**+2**	**+1**	**+0,5**

Таблица $Cooperation\_Threshold_x(\alpha)$ в ранговых шкалах

	1	Ожидаемая компетенция $PC_x(y,\alpha) + T_x(y)^*$					
		2	3	3	5	5	
Рискл. $PR_x(\alpha)$	1	**1**	**1**	**1**	**1**	**1**	**1**
	3	**5**	**4**	**3**	**3**	**2**	**2**
	5	**5**	**4**	**4**	**4**	**3**	**3**

В комментариях работы [13] при сравнении этих таблиц указано:

- если нет риска, то должен быть и минимальный порог сотрудничества (как видим это справедливо для обеих таблиц и более того, в таблице ранговых шкалах отсутствует ошибка, связанная с делением на 0);
- в случае, когда PCx(y,α) = – Tx(y)* в аналитических формулах возникает неопределенность, а ранговых шкалах нет;
- низкий уровень компетенции и высокий риск должны приводить к высокому значению порога сотрудничества, что мы наблюдаем только в ранговых шкалах, а в аналитической модели этого нет (автор считает это одним из главных недостатков);
- при постоянном риске с ростом компетенции порог сотрудничества должен снижаться, что мы наблюдаем в обеих таблицах.

Всего в работе [13] приводится 12 замечаний, связанных в основном с некорректностью вычисления аналитической зависимости. Как можно видеть,

некорректности аналитической модели, описанные в замечаниях, в случае качественных шкал пропадают, а все особенности поведения, связанные с установкой высокого или низкого порога сотрудничества сохраняются.

Заключение

Мы рассмотрели задачу измерения доверия при преобразовании аналитических моделей к описанию в виде иерархических структур и при переходе к качественным шкалам измерений. Это всего лишь одна, хотя и важнейшая, характеристика процесса разрешения конфликта. Хотелось бы отметить, что прозрачность и простота измерения характеристик особенно важна при анализе конфликтных ситуаций, так как она должна быть понятна всем участникам конфликта, что, безусловно, должно способствовать его разрешению.

Литература

1. Алексей Бабанин «Безопасность в облаке: мифы и реальность» «Information Security/Информационная безопасность» №1, 2013.

2. Dan Goodin Security, «2 out of 3 Android apps use private data 'suspiciously» http://www.theregister.co.uk /2010/09/30/ suspicious_android_apps/

3. Светлов В.А.»Аналитика конфликта», СПб., «Росток», 2001.

4. Coser L. The Functions of Social Conflict. London. (3rd edition) 1968. P.8.

5. Д.А. Губанов Обзор онлайновых систем репутации доверия (Институт проблем управления РАН, Москва.

6. Dellarocas C., Resnick P. Online Reputation Mechanisms A Roadmap for Future Research. 2003.

http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.15.514

7. Abdul-Rahman A., Hailes S. Supporting trust in virtual communities // In: Proc. of Hawaii International Conference on System Sciences. 2000.

8. Advogato Trust Metric. http://www.advogato.org/trust-metric.html

9. Mui L., Mohtashemi M., Halberstadt A. A computational model of trust and reputation //System Sciences. 2002. P. 2431-2439.

10. Josang A., Ismail R., Boyd. C. A Survey of Trust and Reputation Systems for Online Service Provision // Decision Support Systems. 2007. Vol. 43. P.618-644.

11. Kamvar S.D., Schlosser M.T., Garcia Molina H.. The EigenTrust Algorithm for Reputation Management in P2P Networks // Proceedings of the 12th international conference on World WideWeb. 2003. P. 640-651.

12. Wagealla, W. and Carbone, M. and English, C. and Terzis, S. and Nixon, P. (2003) A formal model of trust lifecycle management. In: Workshop on Formal Aspects of Security and Trust (FAST2003) as part of the 12th Formal Methods Europe Symposium (FM2003), 2003-09-08 - 2003-09-12, Pisa, Italy.

13. Marsh S. Formalizing Trust as a Computational Concept. 1994. Ph.D. dissertation, University of Stirling.

14. Рамеев О.А. «Методы экспертных оценок. Курс лекций» Москва 2004.

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

THE CONCEPT OF «TRUST» IN CYBER CONFLICT MODELING

Today the concept of "trust" is more and more often used when discussing the problem of cyberspace relations (the Internet, social networks, financial transactions, etc.) gradually replacing such terms as "reliability", "protectability", "security" (and their measurable parameters). Furthermore a number of experts believe that the concept of "trust" can completely replace the conventional notion of security and its characteristics.

This is primarily due to economic issues: the sale of hardware, software, services, data, and other goods and services in cyberspace when the buyer often have no access to objective characteristics of the goods and services he/she purchases.

Overconfidence in cyberspace may prove to be unsafe. In particular, the study conducted by researchers from the University of Pennsylvania and Duke University along with Intel Labs® proofs that two-thirds of Android® applications track dialed numbers, gather information on the geographic location of the device (a cellphone, tablet computer, etc.) and carry out other "suspicious" operations with user's personal data.

It will therefore be worthwhile to give a more precise definition to the notion of "trust" and identify its role in terms of emergence, development and elimination of cyber-conflicts.

Cyber-Conflicts as Determined by the Unified Theory of Conflict

The Unified Theory of Conflict (UTC) [3] views a conflict as a dialectical contradiction which sets the system in motion. The results of a conflict are either synergy or antagonism.

In the case of synergy all the interacting systems are linked to each other in a directly proportional relationship. Therefore, synergy represents a symmetrical reinforcement (or weakening) of the interacting systems. In other words, synergy is a type of coexistence (collaboration, merging into one system) of systems or elements of a system when their parameters get reinforced or weakened simultaneously.

Antagonism, often understood as a conflict situation, represents a type of coexistence of elements of a system when the changes in the properties of the system elements go in different directions. It reasonable to say that antagonism joins elements into one system while separating them onto two poles (coalitions) in such a way that the elements in each coalition are linked to one another through a direct relation while maintaining an inverse relation to the elements in the opposite coalition.

Interactions (including conflicts) in the cyberspace have their own peculiar properties. Very often the so called cyber-conflicts are in fact no less than cyber-wars. For instance, one can recall the recent cyber-attack (or cyber-conflict) that took place between activists of two groups: Spamhaus (London/Geneva) and Cyberbunker (the Netherlands). In essence this conflict is an example of antagonism between economic interests of spammers and anti-spammers. The conflict could have been avoided altogether if the spamming activity had a more robust legal barriers or, alternatively, if barriers to dissemination of any information were removed.

Interacting parties in the cyberspace (including parties in conflict) are represented by users (possibly joined through commercial, public, or government organizations), providers (of services, communication, content, etc.), as well as software and hardware and thus their respective manufacturers and developers.

In the proposed model all participants, the causes and the subject matter of a conflict are interlinked with positive (cooperation, accord) or negative relations. Analysis of the model helps to identify a conflict situation and resolve it by replacing negative relations with positive ones and vice versa.

The Role of Trust in Cyber-Conflicts

Considering the fact that SYNERGY means cooperation and ANTAGONISM means confrontation, the necessary prerequisite for a conflict situation is TRUST which is essential for cooperation and MISTRUST which appears when relations begin to show antagonism.

Under the UTC both synergy and antagonism may be acceptable as results of a conflict situation. An obvious solution will be to build up trust to promote cooperation, yet, although less obvious, excessive trust might also be reduced to diminish negative effects of antagonism.

As an example of the first approach we can consider software and hardware with a good record of practical application and open marketing policies offered by their developers.

An example of the second approach is excessive (unreasonable) trust exercised by users of social networks and other online services which causes leaks of personal data and financial losses.

Both cases require special methods and means of measuring the level of trust.

Trust Models (Metrics)

Over the recent years various mechanisms for measuring trust (reputation) have been in use which is especially important for virtual communities and systems of electronic commerce [5]. The problem of trust and reputation in online systems is the topic of many studies [6] conducted in economics (building up reputation, social learning), computer science (computational models for trust and reputation, scalability, distribution and security of computing operations), sociology and psychology (rationality, the importance of emotional and cognitive factors), management science (the role of reputation/trust in marketing, brand building, etc.) and political science (the effect of reputation on public opinion).

Simple summation or the average value

The reputation is represented by the sum of the numbers of positive and negative comments, an example of this approach in use may be given by eBay. This method is primitive and the resulting reputation values are rather a rough approximation. The advantages of this method, however, are transparency and clarity for the end-user. Epinions and Amazon apply more complex counting algorithms with weighted values (the weights are determined based on the reputation, the time of valuation, distance, etc.)

Aggregators of trust values

Trust and reputation as applied to e-commerce and social networks may be evaluated through a number of mathematical aggregators:

- Abdul-Rahman and Hailes – the graph theory [7];
- Advogato Trust Metric – network flows [8];
- Bayesian approach (based on the beta distribution function [9] and the subjective logic model [10]);
- the lattice model [12].

In the above list, the Abdul-Rahman and Hailes model and the lattice model focus not on the quantitative, but qualitative indicators of trust (which is more natural and convenient for the estimate).

Analytical relationship model

S.Marsh has proposed a more general formalization of trust in his research

[13]. He suggests a set of variables and such their arrangement as to arrive at one trust value within the range of [-1, 1]. Since this will be the model used hereinafter, we provide the notation and relationships for the base, overall and situational trust values depending on the values of knowledge (expertise), importance and usefulness in a particular situation:

Description	Notation	Range of values
Situations	$\alpha\ \beta\ \gamma\ \delta\ \varepsilon$	
Participants (actors, agents)	*a, b, c*	
Knowledge (e.g. x knows y)	$K_x(y)$	0, 1
Importance (i.e. importance of situation α for x)	$I_x(\alpha)$	[0,+1]
Usefulness (i.e. usefulness of situation α for x)	$U_x(\alpha)$	[-1,+1]
Base trust (i.e. gullibility of x)	T_x	[-1,+1)
Overall trust (x trusts y)	$T_x(y)$	[-1,+1)
Situational trust	$T_x(y,\alpha)$	[-1,+1)
Cooperation threshold (in situation α)	$CT_x(\alpha)$	
Presumed risk	$PR_x(\alpha)$	[0,1]
Presumed competence	$PC_x(y,\alpha)$	[0,1]
Presumed usefulness	$PU_x(y,\alpha)$	[0,1]

The above parameters are linked through a following relationship:

$$T_x(y,\alpha)=U_x(\alpha)\cdot I_x(\alpha)\cdot T_x(y)^*$$

or through a more complex relationship:

$$T_x(y,\alpha)=(U_x(\alpha)+T_x(y)^*)\cdot I_x(\alpha)\cdot T_x(y)^{*\,x},$$

where

$T_x(y)^*$ represents the value of trust x has for y (a mean trust value for all possible situations or, in other words, reputation);

$T_x(y)^{*\,x}$ represents the subjective value of trust of x for y (mean trust value taking into account the knowledge x has of y).

The model by S.Marsh assumed that the above values may change over time. It makes an allowance for a certain “depth” of memory, and yet results in more complex relationships which shall not be considered in this document here.

The trust values are assessed to assist an agent in making the decision whether to interact with another agent by comparing against a certain threshold value. Cooperation between x and y in a given situation α is possible when the situational trust is above a certain threshold value:

$T_x(y,\alpha)$ > Cooperation_Threshold$_x(\alpha)$ ⟹ cooperation is possible, where the cooperation threshold Cooperation_Threshold$_x(\alpha)$ is calculated, for instance, based on the presumed risk and the presumed competence and the importance of the situation:

Cooperation_Threshold$_x(\alpha) = (PR_x(\alpha) / PC_x(y,\alpha)) \cdot I_x(\alpha)$

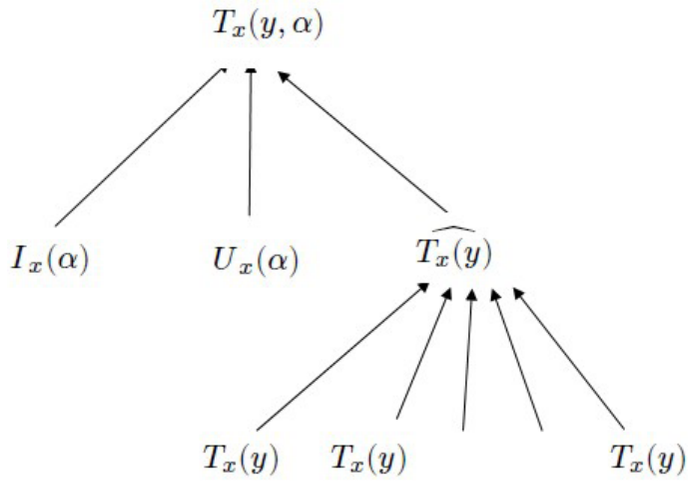
or more precisely:

Cooperation_Threshold$_x(\alpha) = (PR_x(\alpha) / (PC_x(y,\alpha) + T_x(y)^*)) \cdot I_x(\alpha)$

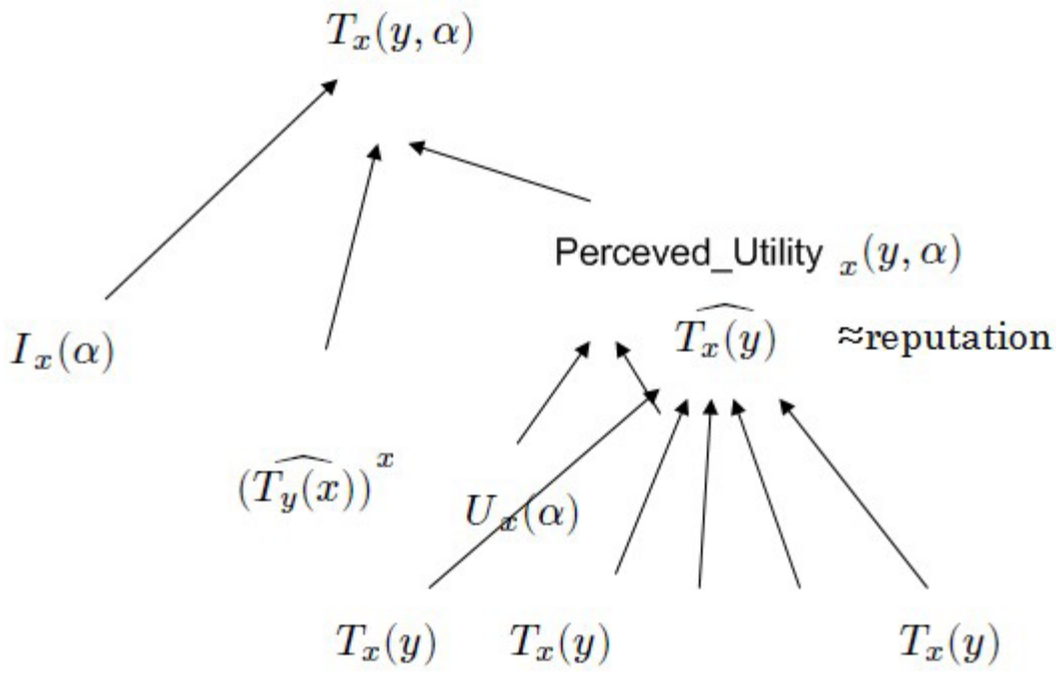
Measurement Model for Qualitative Scales

Using the above analytical model we will demonstrate how to build a model accounting for changes of primary parameters in qualitative scales. In that case the resulting trust value will no longer be in the range [-1, 1], but will be expressed in terms of a quality scale (e.g.: “very poor”, “poor”, “satisfactory”, “good”, “excellent”). We shall hereinafter use a scale of ranks with *n* number of grades.

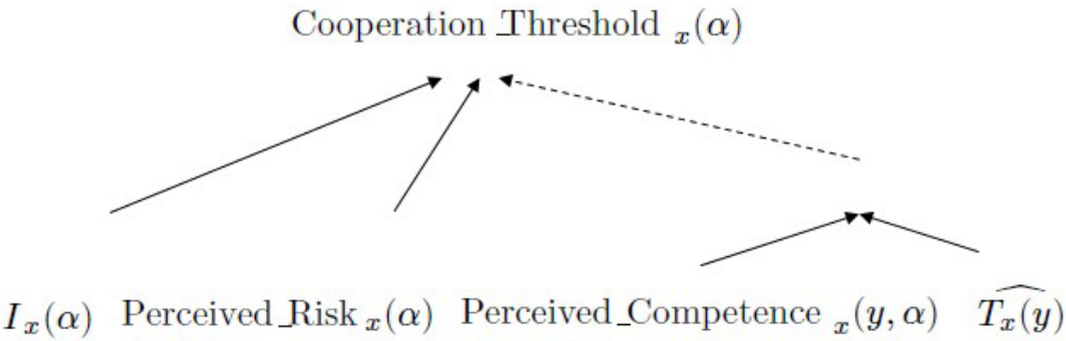
Assuming that all of the above values are expressed through the same qualitative scale (the trust and mistrust values are to be considered separately) the above analytical relationships may be represented as shown below:



or, accordingly:



for the cooperation threshold:



Such hierarchical structures were previously processed (e.g. [14]) using various aggregation and scale transformation techniques: lexicographical ordering (ordering relation of Cartesian product of sets), the method of the rank sums, etc. Since our hierarchical structures are built on analytical expressions, it is advisable to use scale convolutions that correspond to the arithmetic operations keeping the same scale graduation.

In the general case, the problem of building such convolutions represents a linear order problem with Cartesian product of linearly ordered sets of the same dimension *n* and classifying the product elements under *n* equivalence classes. Such Cartesian product induces a partial order relation:

$$(i,j) \geq (k,l) \iff i \geq k \ \& \ j \geq l ,$$

where *i,j,k,l* are the indices of the linearly ordered sets and their Cartesian product.

Additive convolutions which satisfy the induced partial order relation can be obtained by ordering of the rank sum and product multiplicative.

Examples of the multiplicative (x) and additive (+) convolutions for rank scales with graduation of 5 are shown below:

x	1	2	3	4	5
1	1	1	1	1	1
2	1	2	2	2	2
3	1	2	3	3	3

+	1	2	3	4	5
1	1	2	3	4	5
2	2	2	3	4	5
3	3	3	3	4	5

For the operations of subtraction and division the respective convolutions are less obvious. In such case the ordering relation for one of the linearly ordered sets is reversed which changes the partial order relation of the Cartesian product of sets accordingly:

$$(i,j) \geq (k,l) \iff i \leq k \;\&\; j \geq l\,,$$

where *i,j,k,l* are the indices of the linearly ordered sets and their Cartesian product.

Examples of convolutions of rank scales with graduation of 5 for the operations of division (/) and subtraction (-) respectively based on the ordering of the quotient and difference of the ranks satisfying the new order relation for the Cartesian product of sets are given below:

/	1	2	3	4	5
1	3	1	1	1	1
2	5	3	2	2	2
3	5	4	3	2	2

-	1	2	3	4	5
1	3	2	1	1	1
2	4	3	2	1	1
3	5	4	3	2	1

Although the proposed methods of convolution of scales can be applied to scales with an arbitrary number of gradations, the gradation number presented above is convenient for practical calculations as demonstrated below.

Let us now compare the results of the analysis of the modified formula for Cooperation_Threshold$_x(\alpha)$ given by S.Marsh in his model [13] with the data obtained from the transition to the qualitative scales when $I_x(\alpha)=1$.

Values of the Cooperation_Threshold$_x(\alpha)$, (Model)

		-1	Presumed competence $PC_x(y,\alpha) + T_x(y)^*$				
		-0,5	0	+0,5	+1	+2	
$PR_x(\alpha)$	0	**0**	**0**	**∞**	**0**	**0**	**0**
	+0,5	**-0,5**	**-1**	**∞**	**+1**	**+0,5**	**+0,25**
	1	**-1**	**2**	**∞**	**+2**	**+1**	**+0,5**

Values of the Cooperation_Threshold$_x(\alpha)$, (Rank scales)

		1	Presumed competence $PC_x(y,\alpha) + T_x(y)^*$					
		2	3	3	5	5	
$PR_x(\alpha)$	1	**1**	**1**	**1**	**1**	**1**	**1**
	3	**5**	**4**	**3**	**3**	**2**	**2**
	5	**5**	**4**	**4**	**4**	**3**	**3**

As regards the comparative analysis of the tables the commentary provided in the study [13] indicates the following:

in the absence of risk the cooperation threshold must be minimum (true for both tables, no math error in the rank scales table for no division by 0);

when $PC_x(y,\alpha) = -T_x(y)^*$ the value in the analytical formulas is not defined, while the corresponding value in the rank scales is;

low values of competence and high values of risk must result in a high cooperation threshold which is observed only in rank scales and is altogether absent in the analytical model (the author considers this to be one of their main drawbacks);

when the competence value is growing while the risk values remains a constant the cooperation threshold should decrease which can be observed in both tables.

The study [13] offers the total of 12 comments which are mostly related to inconsistencies of calculating the analytical relationship. As illustrated above the inconsistencies of the analytical model provided in the commentary disappear after transition to the qualitative scales while preserving all of the behavioral characteristics relating to the high and low cooperation threshold.

Conclusion

We considered the problem of measuring the level of trust when representing analytical models as hierarchical structures and when applying qualitative measurement scales. This is just one, albeit a very important characteristic of the conflict resolution process. It is worthwhile to note that transparency and simplicity of measuring parameters is of a particular importance when analyzing conflict situations as it must be clear to all parties to the conflict which then, of course, makes its resolution an easier task.

Bibliography

1. Alexei Babanin *Cloud Security*: *Myths and Realities*. Information Security/Информационная безопасность #1, 2013.

2. Dan Goodin Security, «2 out of 3 Android apps use private data 'suspiciously»

http://www.theregister.co.uk /2010/09/30/ suspicious_android_apps/

3. Svetlov V.A. *Analysis of A Conflict*, St. Petersburg. Rostok, 2001.(in Russian)

4. Coser L. *The Functions of Social Conflict*. London. (3rd edition) 1968. P.8.

5. D.A. Gubanov. *Overview of Online Reputation/Trust Systems*. The Institute of Control Sciences, Russian Academy of Sciences, Moscow. (in Russian)

6. Dellarocas C., Resnick P. *Online Reputation Mechanisms A Roadmap for Future Research*. 2003.

http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.15.514

7. Abdul-Rahman A., Hailes S. *Supporting trust in virtual communities* // In: Proc. of Hawaii International Conference on System Sciences. 2000.

8. *Advogato Trust Metric*. http://www.advogato.org/trust-metric.html

9. Mui L., Mohtashemi M., Halberstadt A. *A computational model of trust and reputation* //System Sciences. 2002. P. 2431-2439.

10. Josang A., Ismail R., Boyd. C. *A Survey of Trust and Reputation Systems for Online Service Provision* // Decision Support Systems. 2007. Vol. 43. P.618-644.

11. Kamvar S.D., Schlosser M.T., Garcia Molina H.. The EigenTrust *Algorithm for Reputation Management in P2P Networks* // Proceedings of the 12th international conference on World WideWeb. 2003. P. 640-651.

12. Wagealla, W. and Carbone, M. and English, C. and Terzis, S. and Nixon, P. (2003) *A formal model of trust lifecycle management*. In: Workshop on Formal Aspects of Security and Trust (FAST2003) as part of the 12th Formal Methods Europe Symposium (FM2003), 2003-09-08 - 2003-09-12, Pisa, Italy.

13. Marsh S. Formalizing *Trust as a Computational Concept*. 1994. Ph.D. dissertation, University of Stirling.

14. Rameev O.A. *Methods for Expert Evaluations*. A Course of Lectures. Moscow 2004. (in Russian)