К российско-американскому двустороннему сотрудничеству в сфере кибербезопасности

ОЛЕГ ДЕМИДОВ, ВИТАЛИЙ КАБЕРНИК, ЕЛЕНА ЧЕРНЕНКО,
ТОМАС РЕМИНГТОН & КРИС СПИРИТО

ДОКЛАДЫ РАБОЧЕЙ ГРУППЫ ПО БУДУЩЕМУ РОССИЙСКО-АМЕРИКАНСКИХ ОТНОШЕНИЙ
ВЫПУСК 7
МАЙ 2016 Г.

us-russiafuture.org

WORKING GROUP ON THE FUTURE OF U.S.- RUSSIA RELATIONS
РАБОЧАЯ ГРУППА ПО БУДУЩЕМУ РОССИЙСКО-АМЕРИКАНСКИХ ОТНОШЕНИЙ

К российско-американскому двустороннему сотрудничеству в сфере кибербезопасности

ОЛЕГ ДЕМИДОВ, ВИТАЛИЙ КАБЕРНИК, ЕЛЕНА ЧЕРНЕНКО,
ТОМАС РЕМИНГТОН & КРИС СПИРИТО

ДОКЛАДЫ РАБОЧЕЙ ГРУППЫ ПО БУДУЩЕМУ РОССИЙСКО-АМЕРИКАНСКИХ ОТНОШЕНИЙ
ВЫПУСК 7
МАЙ 2016 Г.

us-russiafuture.org

WORKING GROUP ON THE FUTURE OF U.S.- RUSSIA RELATIONS
РАБОЧАЯ ГРУППА ПО БУДУЩЕМУ РОССИЙСКО-АМЕРИКАНСКИХ ОТНОШЕНИЙ

Рабочая группа по будущему российско-американских отношений

Рабочая группа по будущему российско-американских отношений объединяет экспертов из ведущих американских и российских организаций для решения сложнейших вопросов двусторонних отношений обеих стран. Объединяя новое поколение ученых в дискуссиях и обсуждениях, она следует цели – проведение инновационного анализа и выработка стратегических рекомендаций, наиболее точно отражающих общие принципы, объединяющие США и Россию, которые часто страдают от взаимного недоверия. Мы убеждены, что наш уникальный истинно двусторонний подход обладает наилучшими перспективами для поднятия на новый уровень взаимного понимания и снятия разногласий между нашими странами.

Опорной точкой Рабочей группы в США является Центр российских и евразийских исследований им. Дейвиса Гарвардского университета. С российской стороны главными партнерами выступают Национальный исследовательский университет «Высшая школа экономики» (факультет мировой экономики и мировой политики), а также Совет по внешней и оборонной политике.

Рабочая группа по будущему российско-американских отношений выражает благодарность Корпорации Карнеги (Нью-Йорк), Национальному исследовательскому университету «Высшая школа экономики», и г-ну Джону Когану за финансовую поддержку деятельности Рабочей группы, включая издание настоящего доклада.

Ответственность за выводы, сделанные в настоящем докладе, а также выраженные в нём мнения, несут авторы настоящего доклада.

Вопросы просьба направлять по адресу:

Working Group on the Future
of U.S.-Russia Relations
c/o Kathryn W. and Shelby Cullom
Davis Center for Russian and Eurasian
Studies
Harvard University
1730 Cambridge St., Suite S301
Cambridge, MA 02138
Тел.: (617) 496-5684
Факс: (617) 495-8319
http://us-russiafuture.org

Рабочая группа по будущему
российско-американских отношений
Центр комплексных европейских и
международных исследований
Факультет мировой экономики и
мировой политики НИУ ВШЭ
Москва, ул. Мытная 46 стр. 6, офис 209
Тел. (495) 772-95-90 * 22187
Факс (495) 771-32-52
E-mail dsuslov@hse.ru
http://us-russiafuture.org

Полный текст настоящего доклада на русском и английском языках находится на странице: http://us-russiafuture.org/publications. В наличии есть ограниченное количество печатных экземпляров. Чтобы заказать экземпляр, напишите нам по адресу: info@us-russiafuture.org.

Содержание

Краткое резюме

В последние годы динамика международного сотрудничества и конфликтов в киберпространстве находится в центре внимания национальных правительств и экспертного сообщества всего мира. Россия и Соединенные Штаты часто расходились во мнениях при определении сути проблемы. Россия делает акцент на «международной информационной безопасности», в то время как США считают киберпреступления, кибершпионаж и кибертерроризм основными угрозами в этой сфере и поэтому предпочитают термин «кибербезопасность» и сфокусированность на защите компьютерных сетей и ресурсов. Поэтому воодушевляет тот факт, что в июне 2013 г. стороны пришли к согласию по поводу необходимости сотрудничества в борьбе с «угрозами при использовании информационно-коммуникационных технологий (ИКТ) в контексте международной безопасности». Последующие мероприятия способствовали дальнейшему прогрессу в развитии сотрудничества. В этом рабочем докладе мы попытаемся выделить некоторые вызовы, а также возможности для российско-американского двустороннего сотрудничества в сфере кибербезопасности.

Кибербезопасность ставит перед нами в определенном смысле уникальные трудности, когда речь идет о сотрудничестве. Теории стратегических конфликтов и безопасности, выработанные в период гонки ядерных вооружений, нельзя просто перенести в киберпространство. Некоторые эксперты, например, сомневаются в том, что доктрины сдерживания и принципы проверки соблюдения соглашений применимы в киберпространстве. Проблема определения источника атаки – еще серьезнее. Атака может происходить практически мгновенно и без всякого предупреждения.

Кроме того, российская и американская стороны склонны подходить к проблеме кибербезопасности с разных точек зрения. Российские власти обычно делают акцент на принципе суверенного контроля над всей информационно-коммуникационной сферой. Россия рассматривает кибероружие по сути как средство первого удара, которое бесполезно, если не применяется на ранних стадиях конфликта. Соединенные Штаты, напротив, отвергают «безопасность информации» как основополагающий принцип и придерживаются идеи, что Интернет должен быть «открытым, безопасным, надежным и обеспечивающим взаимодействие». США разделяют действия в киберпространстве на легитимные и нелегитимные: к нелегитимным формам они относят шпионаж со стороны правительств и компаний с целью получения коммерческих секретов, а также попытки преступных (в том числе террористических) организаций нанести ущерб ИКТ-инфраструктуре. Соединенные Штаты принимают тот факт, что правительства будут заниматься шпионажем в интересах национальной безопасности, а также будут предпринимать попытки повлиять на общественное мнение в конкретных странах, вплоть до свержения находящихся у власти режимов. США выступают за международное сотрудничество в целях предотвращения преступных атак на критически важную ИКТ-инфраструктуру, а

также за запрет шпионажа по коммерческим мотивам, и им удалось найти точки соприкосновения с Россией и другими странами для достижения соглашений по этим аспектам.

Обе стороны признают потенциальную опасность, которую кибератаки могут представлять для национальной инфраструктуры – электроэнергетики, плотин, водоснабжения и канализации, нефте- и газодобывающего оборудования, телекоммуникационных сетей. Опасность крупномасштабной атаки на критически важные объекты инфраструктуры чрезвычайно высока. По этой причине киберпространство является не только виртуальным, с ним связана физическая инфраструктура, касающаяся всех людей.

Российские власти также обеспокоены возможностью вмешательства США в управление основной инфраструктурой Интернета, вплоть до лишения России доступа к ней. Хотя запланированная на середину 2016 г. реформа ICANN (Корпорация по управлению доменными именами и IP-адресами в Интернете) должна вывести технические функции ICANN из-под надзора правительства США и превратить ее в саморегулируемый международный орган, опасения России полностью не сняты.

Мы полагаем, что к этим аспектам киберпространства нужно подходить как на двустороннем, так и на многостороннем уровне. Мы даем шесть рекомендаций для двустороннего российско-американского сотрудничества в сфере кибербезопасности:

a. соглашение по четкому определению пределов атак на критически важную инфраструктуру, когда в ответ может быть нанесен контрудар с применением кибер- или других типов оружия;

b. соглашение по набору информации, которой предполагается обмениваться в случае кибератаки – например, по аналогии с реагированием на биологическую атаку;

c. запрещение автоматического ответного удара – в том числе с использованием конвенционального оружия – в случае кибератак;

d. запрещение атак на основные элементы Интернет-инфраструктуры другого государства;

e. совместная оценка инфраструктуры управления Интернетом (UIS, IANA, DNS RZM), чтобы выяснить, адекватно ли учитываются интересы и вклад всех участников после реформирования ICANN;

f. более широкая международная дискуссия по кибербезопасности за рамками двустороннего взаимодействия России и США – например, под эгидой Группы правительственных экспертов ООН по достижениям в сфере информации и телекоммуникаций в контексте международной безопасности (UNGGE).

Мы полагаем, что в долгосрочной перспективе необходим имеющий обязательную силу международный договор, который обеспечит соблюдение этих норм. Двусторонние нормы, которые мы предлагаем, могут послужить моделью для подобного многостороннего соглашения.

История вопроса

В последние годы динамика международного сотрудничества и конфликтов в киберпространстве находится в центре внимания национальных правительств и экспертного сообщества всего мира. Кибербезопасность – одна из тем, по которым Россия и США ведут активные переговоры, иногда разочаровывающие, иногда плодотворные. Разногласия между США и Россией начинаются на концептуальном уровне. США и их союзники считают, что киберпреступность, кибершпионаж и кибертерроризм являются главными угрозами в этой сфере, поэтому они используют термин «кибербезопасность» и сосредоточены на защите компьютерных сетей и ресурсов. Россия тоже озабочена этими угрозами, но одновременно ее беспокоят и вопросы контента: Москву волнует использование новых технологий для ведения информационной борьбы и дестабилизации режимов. Поэтому Россия, как и некоторые другие страны (в том числе Китай), подчеркивает суверенность информационного пространства, что должно лишить потенциального противника возможности проводить наступательные и психологические операции внутри страны. Вследствие этого Россия обычно говорит о «международной информационной безопасности» и делает акцент на политической и идеологической конфронтации в киберпространстве.[1] Разница в подходах мешает достичь согласия в определении сути проблемы.[2]

Кибербезопасность – одна из тем, по которым Россия и США ведут активные переговоры, иногда разочаровывающие, иногда плодотворные.

Тем не менее, несмотря на эти противоречия, Россия и США в конечном итоге пришли к согласию по терминологии, что позволило им 17 июня 2013 г. «на полях» саммита G8 в Северной Ирландии подписать соглашение, касающееся «вопросов угроз в сфере использования ИКТ в контексте международной безопасности».[3] Стороны договорились о следующем:

a. установить прямые защищенные линии связи между Москвой и Вашингтоном, которые будут использоваться в случае угроз безопасности, связанных с использованием ИКТ; речь идет о прямых контактах между Федеральной службой безопасности (ФСБ) России и Центральным разведывательным управлением (ЦРУ) США в случае киберугроз;

b. разрешить использование «горячих линий» на базе национальных центров по уменьшению ядерной опасности (НЦУЯО) для оповещения о киберугрозах, включая предупреждение о намеченных киберучениях или происходящих кибератаках;

c. обеспечить скоординированную работу групп экстренной готовности к компьютерным инцидентам (CERT) двух стран, т.е. специалистов, которые расследуют и противодействуют атакам на объекты критической ИКТ-инфраструктуры.

---

[1] Концепцию Конвенции по обеспечению международной информационной безопасности МИД РФ можно найти на http://archive.mid.ru//bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument.

[2] Глоссарий терминов, связанных с киберпространством приводится в Приложении А.

[3] Oleg Demidov, "U.S.-Russian CBMS in the Use of ICTS: A Breakthrough with an Unclear Future," *Security Index*, vol. 20 nos. 3–4 (108–9) (2014), pp. 69–80

Вскоре после подписания этого соглашения появилась информация о масштабной прослушке телефонов и отслеживани Интернет-переписки граждан и правительств, которые осуществлялись спецслужбами США. Источником информации стал Эдвард Сноуден, бывший сотрудник фирмы-подрядчика, работавшей с Агентством национальной безопасности (АНБ) США. Вскоре после того как США выдвинули обвинения против Сноудена, российские власти предоставили ему убежище. Такое развитие событий ослабило интерес России и США к дальнейшему сотрудничеству в киберсфере.

После свержения поддерживаемого Москвой правительства Виктора Януковича на Украине российские власти приложили все усилия, чтобы Крым стал субъектом Российской Федерации, и начали оказывать поддержку сепаратистам, воюющим против украинского правительства в восточных областях страны. Все это еще больше осложнило двусторонние российско-американские отношения. США и их союзники ответили введением экономических и финансовых санкций против России. Российско-американские отношения оказались на самом низком уровне за несколько десятилетий. Соединенные Штаты приостановили обсуждение вопросов, связанных с кибербезопасностью, с Россией. Однако ни одна из сторон не пытается аннулировать соглашение 2013 г.

Несмотря на очевидные препятствия на пути к сотрудничеству в сфере кибербезопасности, члены данной рабочей группы полагают, что здесь, как и в других сферах, которые мы определили в последние годы, оба государства выиграют от согласования определенных базовых правил. Мы считаем возможным и желательным придерживаться соглашения 2013 г. и возобновить сотрудничество, чтобы не допустить нанесения катастрофического ущерба национальной ИКТ-инфраструктуре двух стран. Разумеется, мы понимаем опасения обеих сторон, что обмен информацией об уязвимых точках ИКТ-инфраструктуры может позволить противнику использовать эти сведения для наступательной операции. Поэтому конструктивное сотрудничество потребует соглашения о сути информации, которой можно обмениваться до и после предполагаемых атак, а также подходов к обеспечению конфиденциальности информационного обмена.

Можем ли мы извлечь полезные уроки из опыта двустороннего сотрудничества в сфере контроля и сокращения ядерных вооружений? Гонку ядерных вооружений удалось обуздать благодаря серии соглашений, начиная с Договора о запрете ядерных испытаний, подписанного советским лидером Никитой Хрущевым и президентом США Джоном Кеннеди в 1963 г., и заканчивая соглашениями по ПРО, ОСВ и СНВ. Эти документы ассоциируются с обязательствами, которые можно проверить с помощью «национальных технических средств» – в частности спутниковых снимков, а также посредством инспекций объектов. Соблюдение этих соглашений обеими сторонами подкрепляют средства проверки, а не доверие. Как в «дилемме заключенного», в интересах обеих сторон сотрудничать, пока есть средства убедиться, что другая сторона тоже сотрудничает. Конечно, каждая сторона признает собственную заинтересованность в том, чтобы избежать риска военной конфронтации, которая может привести к ядерному конфликту. Поэтому способность нанести сокрушительный ответный удар усиливает взаимное сдерживание посредством реальности гарантированного взаимного уничтожения.

Сочетание взаимного сдерживания и проверки выполнения обязательств помогает поддерживать стабильность в гонке ядерных вооружений. С 1970-х гг. обе стороны признают стратегическую стабильность в ядерной сфере желательным исходом.

Однако многие наблюдатели подчеркивают различия между безопасностью в киберпространстве и в сфере ядерных вооружений. Во-первых, термин «кибервойна» включает в себя многочисленные формы потенциального конфликта – война между государствами в киберпространстве, война между государствами с использованием кибероружия в дополнение к другим типам вооружения, а также злонамеренные атаки в киберпространстве, недотягивающие до прямой войны. В этом докладе мы рассматриваем шпионаж как действия, недотягивающие до войны.

Термин «кибервойна» включает в себя многочисленные формы потенциального конфликта – война между государствами в киберпространстве, война между государствами с использованием кибероружия в дополнение к другим типам вооружения, а также злонамеренные атаки в киберпространстве, недотягивающие до прямой войны.

Некоторые эксперты полагают, что в сфере кибербезопасности, в отличие от обычных или ядерных вооружений, ни проверка выполнения соглашений, ни сдерживание невозможны.[4] Проверке соблюдения соглашения по кибербезопасности мешает то, что отследить источник атаки чрезвычайно сложно. Некоторые утверждают, что точно и своевременно определить ответственного за кибератаку невозможно или практически невозможно, и абсолютно невозможно в режиме реального времени. Например, даже если удастся отследить атаку до конкретного IP-адреса, будет трудно определить, какой компьютер использовал этот IP-адрес, не говоря уже о том, кто управлял компьютером. Этим фактом обусловлены опасения, что государства могут ответить на выявленную кибератаку контрударом в иной форме. Т.е. страна, подвергшаяся кибератаке, может в ответ применить обычное или ядерное оружие. Более того, военные стратеги с обеих сторон рассматривают кибервойну как вероятный элемент «гибридной войны» с использованием секретных подразделений, боевиков и отрицаемых атак на коммуникационные сети противника.[5] Поскольку США и Россия сохранили право ответного удара на кибератаки как на обычные акты агрессии, кибератака – будь то самостоятельное событие или элемент гибридной войны – может иметь катастрофические последствия в случае эскалации.

Вполне можно предположить, что хакер-злоумышленник, представляющий криминальную, террористическую или национальную группировку, может атаковать критически важную инфраструктуру США, захватив серверы в третьей стране. Если Соединенные Штаты подвергнутся атаке с серверов, базирующихся в России, посчитают ли они возможным, что атаку спонсируют российские власти? Как отреагируют США? Успешное использование вируса Stuxnet против иранских ядерных центрифуг показывает, что кибероружие существует, применяется и является эффективным, а определить его происхождение трудно. Энекен Тикк предложила «правило ответственности», которое гласит: «тот факт, что кибератака производилась из информационной системы, расположенной на территории определенного государства, является доказательством того, что этот акт связан с этим государством. Если бы правительства приняли это правило, государства несли бы правовую и военную ответственность за атаки, исходящие с их территории. Эта норма заставляла бы государство, с территории которого производилась атака, содействовать ее прекращению и задержанию преступников.[6]

---

[4] Dorothy E. Denning, "Rethinking the Cyber Domain and Deterrence," *Forum* 77, 2015, pp. 8–15.

[5] О том, как военные стратеги России и США понимают – и часто неверно используют – концепцию «гибридной войны, см. Samuel Charap, "The Ghost of Hybrid War," *Survival* 57:6 (December 2015–January 2016), pp. 51–58.

[6] Eneken Tikk, "10 Rules for Cyber Security," *Survival* 53:3 (June–July 2011), pp. 119–32.

Хотя многие полагают, что проверка выполнения обязательств в киберпространстве невозможна, существуют тактики, технологии и процедуры, позволяющие решить эту проблему. Происходит сбор индикаторов, имеющих многомерные отправные точки, что позволяет создать классифицируемый набор характерных вариантов поведения. Далее работа идет в двух направлениях. С одной стороны, специалисты по киберзащите создают классификацию акторов угрозы, «привязав» их к уникальным или общим поведенческим характеристикам. С другой стороны, акторы угрозы, работающие в соответствии с международно признанными нормами поведения (например, государства, занимающиеся эксплуатацией компьютерных сетей и сбором разведданных) могут внести в свои индикаторы определенный набор признаков, что позволяет снизить потенциальную опасность конфликта из-за враждебных атак в киберпространстве. Подобную техническую схему «водяных знаков» Дэйв Айтел в своем посте о политике кибербезопасности описал следующим образом:

В случае выявления крупных проникновений их анализируют команды экспертов. Хотя, разумеется, автоматические системы постоянно ведут поиск признаков проникновения. Наша цель – создать систему, которую может обнаружить команда экспертов, а не автоматическая система. Особенно агрессивное проникновение будет выявляться по сообщению о реагировании, без обращения к первичным данным о проникновении*, что даст определенные политические* преимущества.[7]

Такой подход обеспечит проверку соблюдения соглашений, поскольку любое действие будет иметь определенные «водяные знаки» или теги. Конечно, многие будут говорить, что у акторов угрозы нет стимулов все время быть честными, поэтому проверка соблюдения норм маловероятна. На это мы ответим, что такой вариант ожидаем и на установление доверия потребуется время. Мы также полагаем, что любое соглашение, в котором не будут прописаны индикаторы атаки или проникновения, станет свидетельством того, что актор, представляющий угрозу, на самом деле будет действовать вне рамок соглашений.

Поскольку эффективность режима сдерживания неясна, все больше правительств признают важность установления определенных правил поведения, которые позволят уменьшить риск возникновения, эскалации и разрушительных последствий боевых действий в киберпространстве, а также способствуют углублению сотрудничества по защите Интернета от криминальных и террористических атак. Такие идеи помогли UNGGE подготовить консенсусный доклад для Генерального секретаря ООН, который был представлен 26 июня 2015 г. UNGGE, состоящая из ведущих специалистов по ИКТ от 20 стран, включая Россию и США, пришла к единому мнению по ряду позиций, в том числе:[8]

---

[7] http://cybersecpolitics.blogspot.com/2016/03/a-technical-scheme-for-watermarking.html.

[8] Доклад Группы правительственных экспертов ООН по достижениям в сфере информации и телекоммуникаций в контексте международной безопасности, Генассамблея ООН A/70/174. Текст доклада см. http://www.csistech.org/blog/2015/8/27/un-publishes-latest-report-of-the-group-of-government-experts.

a. государства должны сотрудничать ради предотвращения вредоносного использования ИКТ;

b. государства должны предотвращать использование своей территории в подобных целях;

c. государства должны обмениваться информацией об использовании ИКТ для преступной и террористической деятельности;

d. использование ИКТ для атак на критически важную Интернет-инфраструктуру чрезвычайно опасно, не только для страны, подвергшейся атаке, но и для всего мира, из-за глобальной интеграции Интернета;

e. ИКТ-атаки могут быть очень быстрыми, а найти ответственных сложно;

f. страны, Интернет-инфраструктура которых плохо защищена, представляют угрозу для всего мирового сообщества.

США и Россия вместе с другими ведущими странами признают опасность киберугроз и необходимость установить согласованные практические нормы, которые позволят снизить риск нежелательных конфликтов.

Согласие по этим позициям на четвертом раунде переговоров UNGGE – безусловный успех. Впервые группа смогла представить сильный консенсусный доклад, в котором подчеркивается необходимость выработки норм ответственного поведения государств в киберпространстве. Один из важных принципов консенсуса – идея о том, что право вооруженных конфликтов (LOAC) применимо к киберпространству.[9] Практические предложения, содержащиеся в докладе, включают нормы обеспечения защиты критически важной инфраструктуры, защиты групп реагирования на киберинциденты, а также сотрудничества между государствами в реагировании на запросы, если вредоносная кибердеятельность исходит с их территории. Например, в случае атаки на американскую или российскую систему, исходящей из другой страны, адекватной реакцией со стороны жертвы было бы (через группу экстренной готовности к компьютерным инцидентам [CERT]) направить запрос коллегам в этой стране со следующим текстом: «Мы полагаем, что атака на систему X исходит от системы Y (IP-адрес aa bb cc dd)? Которая находится в вашем IP-пространстве. Есть ли у вас сведения об этой атаке, которые мы могли бы проанализировать вместе?». Затем, в соответствии с соглашением, каждая из сторон могла бы воспользоваться правом проникнуть в ИКТ-пространство предполагаемого атакующего, чтобы попытаться нейтрализовать атаку. Проверкой эффективности соглашения стали бы совместные действия двух акторов по анализу и нейтрализации киберугрозы. Наконец, при расширении действия Вассенаарской договоренности (о противодействии экспорту технологий двойного назначения) на киберпространство, еще одна рекомендованная норма призывает страны бороться с распространением кибероружия, которое может быть использовано в злонамеренных целях.

[9] Применение LOAC в киберпространстве пока наилучшим образом описано в “Tallinn Manual”, опубликованном Центром киберзащиты НАТО в 2013 г. (хотя это неофициальный документ НАТО). “Tallinn Manual” – результат трехлетней работы 20 известных специалистов по международному праву. В документе выделены нормы международного права, которые применимы к боевым действиям в киберпространстве, и обозначены 95 правил для управления подобными конфликтами. Речь идет о таких понятиях, как суверенитет, ответственность государства, jus ad bellum, международное гуманитарное право и право нейтралитета. Российские эксперты высказали критику по многим пунктам документа, но пока не предложили альтернативную точку зрения.

Двусторонне российско-американское соглашение 2013 г. и консенсусный доклад UNGGE 2015 г. свидетельствуют о том, что США и Россия вместе с другими ведущими странами признают опасность киберугроз и необходимость установить согласованные практические нормы, которые позволят снизить риск нежелательных конфликтов. Таким образом, можно предположить, что для киберпространства, как и для других сфер национальной безопасности, можно согласовать определенные правила, регулирующие поведение суверенных государств, которые пойдут на пользу их национальным интересам.

Оценка перспектив российско-американского сотрудничества

И двустороннее соглашение 2013 г., и доклад UNGGE 2015 г. требуют разработки деполитизированных норм, приемлемых для всех государств. Однако, хотя оба документа являются значительными шагами вперед на пути к международному сотрудничеству в киберпространстве, тот факт, что эти нормы являются добровольными и декларативными – т.е. не имеют механизмов реализации – уменьшает их эффективность. Заявленным принципам недостает средств, обеспечивающих их выполнение. Мы полагаем, что эффективные соглашения в сфере кибербезопасности должны подкрепляться механизмами взаимной проверки, а также взаимным сдерживанием, которое более 50 лет действует в сфере ядерных вооружений. Соглашения об общих принципах нужны, но этого недостаточно. Поэтому мы считаем, что юридически обязывающее соглашение предпочтительнее мягкого права или гибких норм. Мы убеждены, что детально прописанные меры по укреплению кибербезопасности возможны. Мы выделили шесть сфер возможных соглашений, которые могли бы действовать в мирное время:

a. соглашение об определениях и пределах критически важной инфраструктуры, когда атака может спровоцировать контрудар с применением кибер- или других типов оружия;

b. соглашение о наборе информации, которой нужно обмениваться в случае кибератаки;

c. соглашение о запрещении автоматического ответного удара в случае кибератаки;

d. соглашение о нормах воздержания от атак на основную Интернет-инфраструктуру другого государства;

e. большая прозрачность и проверка управления основной Интернет-инфраструктурой;

f. соглашение о необходимости международного обсуждения вопросов кибербезопасности, например под эгидой UNGGE.

Ниже мы более подробно обсудим потенциальные пункты соглашения. Однако сначала мы должны рассмотреть различия в подходах США и России к кибербезопасности.

С момента начала военных действий на Украине в России стало уделяться меньше внимания Арктике в связи с увеличением конфронтационной риторики в рамках взаимоотношений Восток-Запад.

Российские власти обычно делают акцент на принципе суверенного контроля над всем информационным/коммуникационным пространством.

Российские власти обычно делают акцент на принципе суверенного контроля над всем информационным/коммуникационным пространством. Эта позиция нашла отражение в соглашении, подписанном Россией и Китаем 8 мая 2015 г.[10] Стороны договорились об основополагающем принципе сотрудничества в сфере информационной безопасности, которое касается защиты каждого из государств от атак на социальную, политическую, экономическую и культурную стабильность. В соглашении «информационная безопасность» определяется как защита индивидуумов, общества и государства от угроз и деструктивного воздействия в «информационном пространстве». В соглашение также включен пункт, запрещающий сторонам использовать информационные ресурсы» для атак друг на друга, что можно назвать «пактом о киберненападении».[11] Соглашение также призывает к сотрудничеству посредством обмена информацией и результатами исследований.

Соединенные Штаты – по крайней мере официально – отвергают концепцию «информационной безопасности» как основополагающего принципа. Скорее, американская концепция (как отражено в заявлении Министерства обороны по кибербезопасности 2015 г.) заключается в том, что «США придерживаются идеи открытого, безопасного, надежного и дающего возможность взаимодействовать Интернета, что обеспечивает процветание, общественную безопасность и свободный поток торговли идей».[12] В недавнем докладе Совета по международным отношениям (CFR) также перечислен ряд принципов, которые в целом приняты американским политическим истеблишментом. Авторы доклада исходят из предпосылки, что Интернет должен быть «открытым, глобальным, безопасным и устойчивым».[13] «Открытость» означает максимальный доступ общества к Интернету и минимальную цензуру и вмешательство со стороны государства; «глобальность» подразумевает противодействие фрагментации Интернета на многочисленные национальные интранеты; «безопасность» обозначает возможности государств защищаться от атак; «устойчивость» - это способность коммуникационных систем восстанавливаться после сбоев и атак. Американская точка зрения, нашедшая отражение в докладе CFR, предполагает, что управление Интернетом должно осуществляться правительствами и частными компаниями с учетом интересов всех сторон. В докладе отмечается, что попытки правительств защитить свои национальные домены от реальных или воображаемых угроз извне могут в конечном итоге привести к введению драконовского контроля контента, локализационных норм и даже выделению национальных доменов в отдельные, замкнутые интернеты. США считают важным поддержание саморегулируемого и децентрализованного характера

[10] http://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html. Текст соглашения на русском языке см. http://government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf.

[11] http://blogs.cfr.org/cyber/2015/08/20/the-next-level-for-russia-china-cyberspace-cooperation/.

[12] Доктрина Министерства обороны США по кибербезопасности опубликована в апреле 2015 г. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf, p. 1 (далее в тексте «киберстратегия Пентагона»)

[13] Council on Foreign Relations, “Defending an Open, Global, Secure and Resilient Internet,” Independent Task Force Report No. 70, 2013.

Интернета. Конечно, сегодня эксперты признают, что именно приоритет этих принципов над безопасностью привел к появлению уязвимых точек, которые стали очевидны теперь.[14]

Противоречит ли позиция США поведению страны в киберпространстве? Задокументированные действия США включают масштабный мониторинг внутренних и международных коммуникаций для сбора разведданных,[15] скрытые операции по влиянию на население (например социальная сеть Zun Zuneo на Кубе, которой управляет USAID[16]), а также воздействие на американских операторов телекоммуникаций и соцсетей для достижения политических целей (к примеру, власти США просили Twitter не проводить технических работ во время «зеленой революции» в Иране[17]). США разделяют действия в киберпространстве на легитимные и нелегитимные: к нелегитимным формам они относят шпионаж со стороны правительств и компаний с целью получения коммерческих секретов, а также попытки преступных (в том числе террористических) организаций нанести ущерб ИКТ-инфраструктуре. Соединенные Штаты принимают тот факт, что правительства будут заниматься шпионажем в интересах национальной безопасности, а также будут проводить операции по воздействию на общественное мнение в конкретных странах, вплоть до попыток свергнуть находящиеся у власти режимы. Соединенные Штаты выступают за международное сотрудничество в целях предотвращения преступных атак на критически важную ИКТ-инфраструктуру, а также за запрет шпионажа по коммерческим мотивам, и им удалось найти точки соприкосновения с Россией и другими странами для достижения соглашений по этим аспектам.

США считают важным поддержание саморегулируемого и децентрализованного характера Интернета.

Как отмечалось выше, из-за различия в подходах России и США потребовалось полтора года, чтобы прийти к компромиссу в названии предмета соглашения, хотя его суть уже была принята обеими сторонами. То же самое различие точек зрения препятствует соглашению о роли Международного телекоммуникационного союза (ITU) в управлении Интернетом. На всемирной конференции МСЭ в декабре 2012 г. США выступили против предоставления организации полномочий по регулированию Интернета. 89 стран – в том числе Россия – подписали соглашение, предоставляющее МСЭ подобные полномочия, 54 страны встали на позицию США. И это неудивительно, учитывая, что МСЭ попросил Лабораторию Касперского (российскую компанию, специализирующуюся на кибербезопасности) дать анализ Flame (вредоносная программа, причастность к которой США не доказана).Таким образом, предоставление МСЭ роли регулятора в будущем могло стать источником проблем для США.[18] В результате один набор международных телекоммуникационных норм обязателен для США и поддерживавших их стран, а другой набор норм действует для России и остальных.

---

[14] Важный пример – риск того, что Интернет-трафик может быть украден путем манипулирования пограничнымb межсетевымb протоколами (BGP), которые действуют как децентрализованные диспетчеры данных в Интернете. Их эффективность зависит от готовности всех взаимосвязанных сетей делиться информацией о доступности линий передачи данных. При случайном или намеренном нарушении BGP весь Интернет-трафик идет в одну национальную сеть, переполняя ее и блокируя ее работу, или позволяет враждебному государству или организации нарушить трафик во всей системе. См. серию расследований Крейга Тимберга “Net of Insecurity”, *Washington Post*, 30 мая–5 ноября 2015 г.

[15] http://www.politico.com/story/2015/05/nsa-phone-data-collection-illegal-court-ruling-117725.

[16] http://www.slate.com/blogs/the_world_/2014/04/03/zunzuneo_the_u_s_government_s_bizarre_and_ill_advised_plan_to_build_a_fake.html?wpisrc=burger_bar.

[17] http://www.washingtonpost.com/wp-dyn/content/article/2009/06/16/AR2009061603391.html.

[18] http://www.cyberdialogue.ca/2012/05/cyber-intrigue-the-flame-malware-international-politics.

С другой стороны, хотя Соединенные Штаты выступаю против предоставления МСЭ регулирующих полномочий в Интернете, они поддерживают многостороннее практическое сотрудничество в борьбе с использованием Интернет-технологий в преступных целях. США подписали Конвенцию Совета Европы по киберпреступлениям (Будапештская конвенция, подписана в 2001 г.). Будапештская конвенция обязывает страны расследовать и наказывать преступления, совершенные с использованием компьютера, которые в документы определяются как криминальная деятельность. Конвенцию ратифицировали 39 стран – многие за пределами Европы; Россия и Китай этого не сделали. Правительства этих стран считают, что сотрудничество в борьбе с киберпреступлениями грозит потенциальной потерей суверенитета, поскольку возможен трансграничный доступ к хранящимся компьютерным данным без санкции другой стороны. Присоединение России к Будапештской конвенции могло бы снять подозрения, что власти закрывают глаза на кибератаки на другие страны, совершенные с российской территории (как в случае с волной скоординированных атак на ИКТ-инфраструктуру Эстонии в апреле 2007 г.).

Кибератаки, кибероружие и боевые действия в киберпространстве

Перспектива кибервойны и использования киберпространства для военных целей относительно нова для российских и американских военных экспертов. Вооружённые силы обеих стран разработали доктрины наступательных и оборонительных операций в киберпространстве, признавая, что киберсфера входит в число потенциально милитаризируемых сфер – включая сушу, море и воздух, – где может возникнуть вооруженный конфликт.[19] В обеих странах идут серьезные дебаты о том, какой должна быть всеобъемлющая национальная ответственность в сфере кибербезопасности. Должно ли государство защищать частные компании от атак из других стран? Этот вопрос встал особенно остро в США после многочисленных атак на финансовые учреждения и корпорации (например Sony Pictures). Подобные атаки обходятся очень дорого: по оценкам Лаборатории Касперского, за два года преступники похитили со счетов финансовых учреждений по всему миру $1 млрд.[20]

Военные обеих стран признают потенциальную опасность, которую представляют кибератаки на национальную инфраструктуру – электроэнергетическую систему, плотины, водоснабжение и канализацию, нефте- и газодобывающее оборудование, телекоммуникационные сети. Даже если эти объекты не подключены к Интернету напрямую, устройства автоматизированной системы управления технологическим процессом (АСУ ТП), используемые для дистанционного контроля по защищенным коммуникационным линиям, могут быть взломаны в результате атаки на другие объекты, где функционируют АСУ ТП. Поэтому угроза крупномасштабной и эффективной атаки на критически важную инфраструктуру вполне реальна. В связи с этим киберпространство нельзя считать полностью виртуальным, оно включает физическую инфраструктуру, которая касается всех людей.

Выше мы отмечали сходства и различия, существующие между гонкой ядерного вооружения и угрозой кибервойны. Одно из различий обусловлено тем, что распространение кибероружия происходит гораздо проще, чем распространение ядерных вооружений. Благодаря мерам контроля удалось добиться определенных успехов в замедлении темпов распространения ядерных технологий и материалов. Кроме того, в этой сфере Россия и США ведут успешное сотрудничество. Еще одно различия связано с относительным преимуществом нанесения первого удара. В ядерной гонке угроза нанесения одной из сторон выводящего из

[19] Киберстратегия Пентагона. Россия впервые обнародовала стратегию информационной безопасности в 2000 г. и с тех пор несколько раз обновляла и дополняла ее. В 2013 г. были приняты «Основы государственной политики Российской Федерации в сфере международной информационной безопасности до 2020 г.». См. http://www.scrf.gov.ru/documents/6/114.html. В 2014 и 2015 гг. документ был обновлен. См. https://ccdcoe.org/cyber-security-strategy-documents.html.

[20] http://www.kaspersky.com/about/news/virus/2015/Carbanak-cybergang-steals-1-bn-USD-from-100-financial-institutions-worldwide.

строя первого удара всегда перекрывалась перспективой потенциального ответного удара, который может нанести противник. Эта доктрина побуждала обе стороны укреплять места наземного базирования ракет и рассредоточивать свое вооружение на суше, в море и воздухе. Считается, что в киберпространстве первый удар может быть более быстрым, чем ядерный, и более смертоносным для потенциала ответного удара. С этой точки зрения, соблазн нанести удар первым вносит дестабилизирующий фактор в стратегический баланс. Поэтому ряд экспертов полагает, что доктрина гарантированного взаимного уничтожения не подходит для боевых действий в киберпространстве.

С другой стороны, недавние события, в том числе кража персональных файлов более 22 млн человек из Управления личного состава ВС США, которая, по данным американских властей, осуществлялась из Китая, отражают долгосрочные усилия по сбору информации о правительственных структурах и военнослужащих США, а не деструктивный первый удар.[21] Шпионаж подобного рода может дать противнику более значительное кумулятивное преимущество, чем прямые попытки блокировать работу компьютерных сетей или разрушить их.

Независимо от относительной серьезности угрозы успешного первого кибердара по сравнению с многолетними усилиями по изучению и использованию уязвимых точек в ИКТ-пространстве противника, эксперты обеих сторон согласны в том, что основной стратегический упор должен быть сделан на улучшении защитных возможностей – способности предотвращать деструктивные атаки – и повышении надежности основных систем в случае атаки. Если довести эту логику до крайности, можно предположить, что военные стратеги готовы пойти на отделение национального Интернет-пространства от глобального Интернета в случае ожидаемой или происходящей кибератаки. По сути это означает создание собственного механизма управления корневой зоной системы доменных имен (DNS) – т.е. отдельного национального Интернета или национального интранета. Проще говоря, это позволит, например, России «отключить» Рунет в случае чрезвычайной ситуации и использовать резервную систему, не связанную с глобальным Интернетом.[22] Эксперты отмечают, что Россия использует сотрудничество с другими членами БРИКС для создания подобной параллельной системы.

Россия опасается, что против нее могут быть совершены попытки взять контроль над Рунетом во враждебных целях – например, чтобы разжечь революцию или лишить Россию доступа к собственной ИКТ-инфраструктуре. Эти страхи подпитывает тот факт, что правительство США, а именно Национальная администрация по телекоммуникациям и информации (NTIA) при Министерстве торговли[23] является стороной соглашения с Корпорацией Интернета по

---

[21] Ellen Nakashima, "Officials: Chinese Had Access to U.S. Security Clearance Data for One Year," *Washington Post*, June 18, 2015.

[22] Alexandra Kulikova, "Top 8 Major Trends on the Russian Internet in 2014," *Russia Direct*, December 24, 2014, http://www.russia-direct.org/analysis/top-8-major-trends-about-russian-Internet.

[23] NTIA является органом исполнительной власти (агентством), чья первоочередная обязанность состоит в предоставлениирекомендаций и советов Президенту США по вопросам политики в сфере телекоммуникаций и информаци. Программная деятельность и выработка политик NTIA сконцентрированы прежде всего на расширении и продвижении широкополосного доступа к Интернету в Америке, расширения использования спектра частот всеми пользователями, и сохранение роли Интернета как двигателя непрерывных инноваций и экономического роста. [Источник: NTIA Mission at NTIA website: https://www.ntia.doc.gov/].

распределению имен и адресов (ICANN) о ведении баз данных, которые имеют ключевое значение для функционирования глобального Интернета. Хотя в 2009 г. США передали контроль ICANN, Министерство торговли остается стороной соглашения с ICANN об управлении IANA (Администрацией адресного пространства Интернет) посредством краткосрочных продлений первоначального контракта. Россия опасается, что в чрезвычайной ситуации правительство США может приказать ICANN или частному коммерческому оператору Verisign, который выполняет важные технические функции для ICANN, взять контроль над Рунетом.

В заявлении Минобороны США по кибербезопасности от 2015 г. предполагается, что проблему определения ответственных за атаку можно решить с помощью усовершенствованной экспертизы. В документе содержится призыв разработать потенциал сдерживания, базирующийся на способности отвечать на атаки, успешно защищаться от атак и восстанавливаться после атак. В документе не говорится – и было бы глупо это делать, – что Соединенные Штаты в настоящее время обладают потенциалом «для уменьшения анонимности в киберпространстве и повышения надежности в определении происхождения атак».[24] Вместо этого в документе отмечается, что США «нуждаются» в таких возможностях и «инвестируют в них значительные средства».

Согласно документу Минобороны, перед американскими военными стоят три принципиальные задачи в киберпространстве: защитить собственные системы, защитить страну от серьезных кибератак и обеспечить поддержку американских военных операций (в том числе с использованием кибероружия).[25]

Для России концепция киберпространства как сферы боевых действий подразумевает более широкий взгляд на задачи. Киберпространство рассматривается как сфера всех кибернетических устройств, включая оборудование, программное обеспечение, а также их операторов. Соответственно, российские военные считают оборудование и инфраструктуру, используемые для проведения операций в киберпространстве, частью этого киберпространства. Точно так же люди, которые обслуживают, проводят операции или каким-то иным образом задействованы в киберпространстве, являются частью киберсферы. Поэтому киберпространство не рассматривается исключительно как виртуальное. Оно имеет конкретные физические точки входа. Дата-центры, операторы и коммуникационная инфраструктура рассматриваются как легитимные объекты контроля в киберпространстве.

Поэтому связанные телекоммуникационные сети (например Интернет) и киберпространство – это не одно и то же. Системы управления, такие как комплексы электродистанционного управления для истребителей – включая пилота – рассматриваются как часть киберпространства, даже если находятся на его периферии. Эти системы не подключены к Интернету и никогда не будут подключены из-за несовместимости протоколов. То же самое касается АСУ ТП, которые физически не подсоединены к Интернету и даже могут работать без протоколов стека TCP/IP. В российском понимании все многообразие устройств, систем контроля, отдельных сетей и т.д. является частью киберпространства.

---

[24] Киберстратегия Пентагона, DOD Cyber Strategy, p. 11

[25] Киберстратегия Пентагона, DOD Cyber Strategy, pp. 4–5.

Кроме того, российские военные считают киберсферу частью тесно интегрированного, комплексного пространства боевых действий. В него входят суша, море, воздушное пространство, а теперь еще и кибероперации. Включение киберсферы в интегрированное поле боевых действий отражает прямолинейную логику. Если одна из сторон не обладает преимуществом в какой-либо из составных частей интегрированного пространства боевых действий, она будет использовать свои преимущества в других сферах. Это означает, что сторона, проигрывающая в киберсфере, может и будет задействовать другие пространства боевых действий.

Контролировать распространение кибероружия чрезвычайно сложно, но попытаться это сделать стоит.

Модели эскалации, разработанные для российских вооруженных сил, исходят из того, что сторона, инициировавшая наступательную операцию в киберпространстве, получает превосходство, и противнику будет трудно восстановиться после атаки. Пассивной обороны недостаточно. Поэтому единственное эффективное средство сдерживания – предпринять шаги, чтобы перехватить инициативу с помощью упреждающих наступательных действий. Если эта идея будет актуализирована, эскалация конфликта с боевыми действиями в киберпространстве очень быстро станет сопоставимой с обычными боевыми действиями, а время для замораживания или деэскалации конфликта окажется очень ограниченным.

Соответственно, согласно российской точке зрения, кибероружие создается для нанесения первого удара. Если оно не будет применено на ранних стадиях конфликта, то станет бесполезным, когда конфликт перейдет в стадию классических боевых действий. Иными словами, кибероружие может быть использовано только для полномасштабных глобальных боевых действий между одинаково мощными державами в первые несколько часов конфликта, до того как коммуникационные сети будут нарушены или уничтожены. Глобальный охват и практически мгновенная реакция являются основными характеристиками кибероружия. Эти характеристики ставят кибероружие в один ряд с другими типами стратегического вооружения.

По этой логике даже когда государства работают над улучшением защиты от атак мошенников, они создают милитаризованный киберпотенциал, и этот процесс практически невозможно остановить – как и ядерную гонку вооружений. Контролировать распространение кибероружия чрезвычайно сложно, но попытаться это сделать стоит. Как и попытаться определить пределы ущерба, который может спровоцировать военный ответ. В киберстратегии Минобороны США говорится о необходимости «защищать США и их интересы от кибератак со значительными последствиями». Какие последствия считать «значительными», решает президент, но, согласно документу, они включают «гибель людей, значительный ущерб собственности, серьезные неблагоприятные последствия для внешней политики США и негативное экономическое воздействие на США».[26] В случае с атакой на Sony Pictures в конце 2014 г., которую связали с Северной Кореей, США ответили – по выражению Барака Обамы – «пропорциональной силой». Пропорциональность ответа – одна из правовых норм вооруженного конфликта, которые приняты UNGGE. В этом случае Соединенные Штаты

[26] Киберстратегия Пентагона, DOD Cyber Strategy, p. 5.

официально ввели новые санкции против нескольких северокорейских чиновников, а неофициально могли временно блокировать доступ КНДР к Интернету.[27]

Инцидент с Sony и Северной Кореей ставит на повестку дня два вопроса, напрямую связанных с международным сотрудничеством по кибербезопасности: что такое предельный ущерб национальным интересам страны от кибератаки, который дает основание правительству ответить военными средствами, и насколько правительство должно быть уверено в происхождении атаки, прежде чем предпринять ответные действия против государства или организации? Некоторые наблюдатели высказывают сомнения по поводу действий США в случае с Sony, ставя под вопрос серьезность угрозы для жизненно важных национальных интересов США, а также достаточность доказательств того, что КНДР являлась спонсором атаки, чтобы оправдать ответные действия. Американские власти заявили, что разведданные, на основе которых было определено происхождение атаки, имеют стратегическое значение и их нельзя обнародовать, поэтому экспертное сообщество не может оценить обоснованность действий США. Соединенные Штаты и Россия могли бы применить к боевым действиям в киберпространстве постулат, базирующийся на доктринах эскалации кинетических боевых действий: порог использования наступательного кибероружия в ответ на кибератаку должен быть очень высоким.

Мы не даем оценок о пороге угрозы и определении происхождения атаки, но считаем, что этот случай помогает прояснить значимость вопросов, которые стоят на кону. Двусторонняя и многосторонняя дискуссия о том, что представляют собой жизненно важные национальные интересы в сфере кибербезопасности, поможет увеличить прозрачность принятия решений о применении кибероружия. Мы полагаем, что Россия и США могут договориться о том, что ключевые объекты Интернет-инфраструктуры не должны становиться объектами кибератак, а управление ими должно осуществляться на многосторонней основе. Такая договоренность должна стать центральным элементом следующего соглашения по кибербезопасности между Россией и США.

Норма об обмене информацией об атаках должна стать вторым ключевым элементом следующего соглашения. Здесь следует задействовать другую модель. Вместо того чтобы сравнивать их с ядерной войной, мы можем рассматривать их по аналогии с предполагаемой биологической атакой. В случае предполагаемой атаки с использованием биологического оружия, в том числе террористического характера, различные государственные структуры обычно реагируют по-разному. Правоохранительные органы собирают доказательства для уголовного преследования виновных, засекретив информацию, чтобы не допустить паники и лишить противника каких-либо преимуществ, не демонстрируя ему свою уязвимость. Органы здравоохранения, напротив, действуют максимально открыто, чтобы смягчить последствия атаки. Их приоритет – не преследование и наказание виновных, а ограничение и нейтрализация вспышки. Только после того как вспышка будет остановлена, можно заниматься определением происхождения атаки и необходимых ответных действий. Органы здравоохранения отдают приоритет более широкому обмену информацией о распространении смертельно опасного заболевания, а не ее сокрытию.

---

[27] https://www.washingtonpost.com/world/national-security/why-the-sony-hack-drew-an-unprecedented-us-response-against-north-korea/2015/01/14/679185d4-9a63-11e4-96cc-e858eba91ced_story.html, http://www.wsj.com/articles/u-s-penalizes-north-korea-in-retaliation-for-sony-hack-1420225942.

Обмен информацией об уязвимых точках, выявленных в результате кибератаки, потребует определенного уровня доверия. Как и в сфере обычных и ядерных вооружений, меры укрепления доверия в киберпространстве могут быть основаны на регулярном обмене информацией между правительственными и неправительственными экспертами. Взаимное доверие может быть достигнуто посредством опыта обмена точной информацией о кибердеятельности. Неофициальные (Track Two) дискуссии экспертов могут сыграть полезную роль, дополнив дипломатические каналы.

Аналогичным образом, поскольку сдерживание в сфере кибербезопасности не может быть основано ни на точном определении ответственных за атаки, ни на угрозе эффективного ответного удара (из-за преимущества первого хода),[28] лишение атакующего стратегического преимущества посредством инвестиций в защиту и повышение надежности будет более эффективным, чем сдерживание угрозой контрудара. Отсюда вытекает наша третья рекомендация: обе стороны признают, что идея «запуска по сигналу предупреждения» или автоматического ответного удара должна быть полностью исключена, вместо нее должен действовать постулат лишения преимуществ посредством защиты и повышения надежности. Эдвард Сноуден рассказал о разработке в США подобной программы под названием MonsterMind.[29] Мы выступаем против использования таких механизмов по причинам, изложенным выше. Во-первых, кибератака скорее всего будет замаскирована и пойдет через машины третьей стороны, например зараженные ботами или частные или государственные серверы третьей стороны. Поэтому автоматический ответный удар может привести к военному конфликту со странами, где расположены эти серверы. Во-вторых, ответный удар может непреднамеренно нанести ущерб системам сторонних наблюдателей, например повредить гражданскую инфраструктуру. Таким образом, концепция автоматического ответного удара имеет те же фундаментальные пороки, как и «машина Судного дня» в фильме «Доктор Стрейнджлав».

Поэтому мы рекомендуем сторонам обмениваться информацией об атаках, а не скрывать ее.

---

[28] В теории игр обозначает преимущество, которое получает участник, сделавший первый ход в игре.

[29] http://www.wired.com/2014/08/nsa-monstermind-cyberwarfare/.

Управление глобальной инфраструктурой Интернета

Четвертая сфера рекомендуемых соглашений затрагивает вопросы управления технической инфраструктурой глобального Интернета. Поскольку обеспечение надежности Интернета – общий интерес для России и США, стороны признают значение стабильности, безопасности и отказоустойчивости (SSR) системы уникальных идентификаторов (UIS) Интернета и управления важнейшими процессами, касающимися ее функционирования.

Эти вопросы никогда не входили в повестку дня по кибербезопасности в ее обычном понимании и в настоящий момент не являются предметом двусторонних переговоров России и США. Однако обе стороны заинтересованы в этом вопросе. Кроме того, без конструктивного диалога развитие ситуации в этой сфере может негативно сказаться на обычных операциях в Интернете, затронув основные коммуникации, экономические нужды и даже интегрированность глобального Интернета.

Как отмечалось выше, у Соединенных Штатов исторически сложились уникальные отношения с техническими органами, отвечающими за функционирование этой инфраструктуры на глобальном уровне, включая ICANN и ее техническое подразделение IANA. Международные и внутриамериканские дебаты о роли правительства США в надзоре за функционированием этих технических структур обострились в последние годы, особенно после разоблачений Эдварда Сноудена, хотя они и не связаны напрямую с глобальной инфраструктурой Интернета. В марте 2014 г. начался переходный процесс в сфере надзора за IANA, цель которого – обеспечить передачу надзора за некоторыми критически важными функциями в этой сфере от правительства США глобальному многостороннему органу. ICANN по сути станет саморегулируемой организацией.[30] Новая модель была одобрена в марте 2016 г. на заседании ICANN в Марракеше, ее внедрение должно начаться к осени 2016 г.

В России с 2014 г. вопрос обеспечения стабильности и безопасности инфраструктуры национального сегмента Интернета вышел на первый план по ряду причин. В июле 2014 г. были проведены первые крупномасштабные киберучения Минкомсвязи с участием ФСБ, ФСО, Минобороны, МВД; «Ростелекома», крупнейшего российского интернет-провайдера, Координационного центра национальных доменов .ru/.рф и крупнейшей в России точки обменатрафиком (IXP)[31] MSK-IX. Эти киберучения являются определенной вехой, во-первых, из-за их масштаба и количества задействованных федеральных структур, а также из-за протестированных моделей угроз. Некоторые модели угроз нетипичны для международных – в частности западных – киберучений.

---

[30] "We the Networks," *Economist*, March 5, 2016.

[31] IXP – физические точки, через которые сети обмениваются информацией.

Как рассказал помощник президента Путина Игорь Щеголев в интервью онлайн-порталу Экспертного центра электронного государства 17 октября 2014 г., один из сценариев учений предполагал нарушение работы российского сегмента глобальной Интернет-инфраструктуры в результате «недружественных внешних воздействий». Под таким словосочетанием может подразумеваться кибератака на российскую инфраструктуру, например DDoS-атаки на DNS-серверы, DNS-атаки с лавинообразным усилением ответа, отравление кэша DNS-серверов,[32] нарушение маршрутизации между сетями посредством вброса информации, и т.д.

«Один из основных рисков – целенаправленное отключение России от глобального Интернета».

Общественное обсуждение киберучений и интервью помощника президента главным образом фокусировалось на уязвимости российского сегмента инфраструктуры Интернета вследствие того, что глобальная инфраструктура Сети де-факто управляется иностранным государством, а именно Соединенными Штатами. С этой точки зрения, «недружественные внешние воздействия» могут выходить далеко за рамки кибератак на инфраструктуру. Как отметил помощник президента Щеголев, «один из основных рисков – целенаправленное отключение России от глобального Интернета». Далее он подчеркнул, что управление глобальным Интернетом по-прежнему осуществляют США.

В октябре 2014 г. Совет безопасности России провел закрытое заседание, посвященное обеспечению стабильности, безопасности и устойчивости Рунета в свете киберучений, состоявшихся в июле. После заседания глава Минкомсвязи Николай Никифоров заявил, что Россия будет стремиться к сотрудничеству с партнерами по БРИКС в целях разработки и введения в эксплуатацию резервной критически важной инфраструктуры российского национального сегмента Интернета. В дальнейших публикациях и экспертных дискуссиях в российских СМИ высказывалось мнение, что основной целью этой работы должно стать обеспечение резервных технических возможностей российского сегмента DNS, что позволит системе функционировать автономно в случае серьезного кризиса.

Эту повестку подкрепляли дальнейшие действия Минкомсвязи и других российских госорганов. В марте 2015 г. ведущие российские СМИ сообщили, что министр Никифоров представит правительству закрытый доклад, в котором содержится ряд предложений, направленных на укрепление устойчивости и обеспечение суверенности российского сегмента Интернета. Как сообщалось, эти предложения в основном связаны с ужесточением государственного контроля над критически важными элементами инфраструктуры, включая крупные точки обмена трафиком IXP, обеспечивающие трансграничный обмен трафиком. Одна из IXP – MSK-IX – играет особенно важную роль, обеспечивая ключевую долю трансграничного обмена трафиком в России. Помимо MSK-IX еще две структуры имеют ключевое значение для бесперебойного функционирования российского сегмента Интернета: Координационный центр национального домена (администратор доменов верхнего уровня .ru/.рф) и Технический центр Интернет, который занимается технической поддержкой систем регистрации и делегирования данных доменов верхнего уровня в российском национальном сегменте и тесно связан с Координационным центром. Официально было заявлено, что основная мотивация усилий государства в этой области – «защита Рунета от внешних атак и недружественных воздействий». Однако новых сообщений о статусе доклада и его презентации не поступало.

[32] т.е. заражение вредоносными программами.

В октябре 2015 г. глава российского Интернет-провайдера «ЭР-Телеком» рассказал СМИ об эксперименте, который проводился совместно с Минкомсвязи и Роскомнадзором и моделировал отключение России от глобального Интернета в результате неких «внешних воздействий». По данным СМИ, российские провайдеры блокировали трафик, идущий по основным каналам, связывающим Рунет с глобальными сетями, следуя инструкциям министерства и используя оборудование для глубокойпроверки сетевых пакетов (DPI). Но эксперимент провалился из-за мелких провайдеров: поскольку у них не было DPI-оборудования, они использовали диверсифицированные каналы, включая спутники, и трафик шел через их сети, обеспечивая связь Рунета с глобальным Интернетом. Стоит добавить, что федеральные органы власти опровергли информацию об эксперименте и назвали сообщения «совершенно неверным толкованием» их реальной деятельности.

В апреле 2015 г. на международной встрече по информационной безопасности формата Трек 2 высокопоставленный российский представитель сделал неожиданное заявление. По его словам, если Соединенные Штаты не предпримут шаги по интернационализации механизма управления глобальным Интернетом, Россия гипотетически может начать сотрудничество со своими союзниками с целью разработки автономной трансграничной сети, которая будет иметь независимые от Интернета инфраструктурные элементы. В конечном итоге это будет означать фрагментацию глобального Интернета, что, как отметил представитель, окажет негативное воздействие на трансграничные возможности, которые дает Интернет в сфере услуг, бизнес-процессов и глобальной цифровой экономики. Однако российский спикер подчеркнул, что этот шаг может иметь огромные преимущества с точки зрения безопасности, стабильности, защиты от кибератак и электронного шпионажа для тех государств, которые решат присоединиться к новой автономной сети. Кроме того, современные проблемы кибербезопасности в сочетании с недостатками существующей архитектуры управления Интернетом могут превратить подобный сценарий в «неизбежное зло». По сути это был манифест в пользу концепции, которую принято называть фрагментацией Интернета – архитектурный распад глобальной сети на несколько (или много) полу- или полностью автономных и независимых сегментов.

Исторически разработка Интернета, механизмов его управления и инфраструктуры обусловили создание уникальной модели системы уникальных идентификаторов Интернета (УИИ).[33] На глобальном уровне за безопасное, стабильное и надежное функционирование системы УИИ отвечает техническая структура – IANA (Администрация адресного пространства Интернета). IANA даже не является юридическим субъектом, это техническое подразделение другой структуры – ICANN. В свою очередь ICANN, некоммерческая корпорация, зарегистрированная в штате Калифорния, является стороной контракта о выполнении функций IANA. Сегодня другой стороной контракта является правительство США в лице Национальной администрации по телекоммуникациям и информации (NTIA). В контракте зафиксирован долгосрочный статус-кво: IANA выполняет ряд критически важных бизнес-процессов, обеспечивая функционирование системы уникальных идентификаторов Интернета, под надзором правительства США.

[33] Более подробное рассмотрение системы уникальных идентификаторов (UIS) Интернета можно найти в Приложении B. В Приложении C представлена схема управления Интернетом.

Одним из важнейших бизнес-процессов является управление корневой зоной DNS (RZM). Управление корневой зоной DNS – ключевой процесс для стабильности, безопасности и устойчивости системы УИИ, в настоящее время в нем задействованы несколько ответственных сторон:

a. IANA – оператор, в настоящее время представленный ICANN. Оператор получает, рассматривает и обрабатывает запросы на изменение файла корневой зоны, выполняет техническую проверку, уведомляет операторов о выполнении запросов и вносит изменения в корневую базу данных WHOIS;

b. Администратор, в настоящее время (до завершения полномочий NTIA), представленный NTIA. Администратор проверяет процессы, процедуры и политику, которые осуществляет оператор IANA, разрешает стороне сопровождения вносить изменения в файл корневой зоны по запросу операторов доменов верхнего уровня и разрешает IANA вносить изменения в базу данных WHOIS;

c. Технический менеджер корневой зоны, в настоящее время представленный Verisign. Технический менеджер вносит изменения в файл корневой зоны, генерирует обновленный файл, а также рассылает его по вторичным авторитативным корневым серверам DNS.

Процесс управления корневой зоной включает несколько этапов: отправку запросов на внесение изменений от операторов доменов верхнего уровня, обработку запроса IANA и его отправку на рассмотрение и одобрение в NTIA, одобрение запроса NTIA и его отправку Verisign, техническому менеджеру корневой зоны. Verisign выполняет технические функции в рамках данного бизнес-процесса: генерирует обновленный файл корневой зоны на скрытом первичном мастер-сервере, а затем рассылает его на 13 авторитативных серверов, обозначенных латинскими буквами от A до M. Эти серверы поддерживают корневую зону DNS – верхний уровень в глобальной иерархии системы DNS.

Файл корневой зоны (RZF) содержит информацию обо всех доменах верхнего уровня и связанных с ними IP-адресах. Изменение этих данных в файле приведет к изменениям в глобальном пространстве доменных имен. В контексте киберучений в России в 2014 г. и анализа моделей угроз одна из них теоретически может включать удаление информации о доменах верхнего уровня в зону .ru/.рф из файла корневой зоны. Когда срок действия кеша на корневых серверах DNS истечет, ресурсы этих доменов станут недоступными для пользователей как в России, так и в мире. Получить доступ к этим ресурсам можно будет только напрямую по IP-адресам, что чрезвычайно неудобно для всех категорий пользователей.

В чем заключаются проблемы институционального механизма управления корневой зоной, которые вызывают опасения России и стали лейтмотивом киберучений в 2014 г. и затем обсуждались Советом безопасности РФ?

Во-первых, они не касаются технических параметров системы как таковой. Даже жесткие оппоненты IANA и функционирующей при поддержке правительства США модели глобальной инфраструктуры Интернета признают, что

инфраструктура корневой зоны DNS и ресурсов нумерации достаточно надежна и эффективна, чтобы выдержать самые мощные атаки. Сегодня практически любой корневой сервер DNS имеет многочисленные копии-«зеркала» по всему миру – например, корневой сервер J, оператором которого является ICANN, имеет более 150 «зеркал» на всех континентах, кроме Антарктиды. Инфраструктура глобальной системы распределения IP-адресов также имеет пять Региональных регистратур Интернет (РРИ), каждая из которых отвечает за свой регион (включая Антарктиду). Именно РРИ, а не IANA контролируют присвоение IP и номеров Автономной Систем (ASN)[34] интернет-провайдерам. Некоторые РРИ разрабатывают и осуществляют пользовательскую политику. Наконец, факты свидетельствуют о том, что за исключением нескольких инцидентов в 2002 г., не было зафиксировано злонамереннеых действий (кибератак), которые повлекли бы масштабное нарушение работы инфраструктуры DNS и ресурсов нумерации. Безусловно, имеются определенные изъяны в защите DNS от DDoS-атак (а также использования DNS для генерации DDoS-трафика посредством атаки типа усиления за счет DNS-ответов (DNS Amplification). Серьезные проблемы с безопасностью присутствуют и в глобальной системе маршрутизации, которая основана на Протоколе граничного шлюза (BGP),[35] на этапе разработке которого концепция безопасности отсутствовала как таковая. В конечном итоге все заинтересованные стороны, включая Россию, Китай и другие правительства, понимают, что система УИИ весьма надежна и устойчива.

Поэтому, с российской точки зрения, фундаментальная проблема нынешней системы управления связана не с техническим несовершенством системы УИИ, а скорее с глубоким недоверием к функциям, которые выполняют операторы критически важных бизнес-процессов. Реальная угроза российскому национальному сегменту Интернета, с точки зрения Совета безопасности России и других органов власти, может исходить не от хакеров, которые бы атаковали корневые серверы DNS и удаляли данные о российских доменах верхнего уровня (.ru/.рф) из файла корневой зоны, а от NTIA и федерального суда США, способных выкрутить руки ICANN с помощью правительственных директив и ордеров и заставить IANA предпринять определенные шаги. Такой сценарий угрозы основан на предположении, что IANA и другие операторы глобальной инфраструктуры Интернета при определенных обстоятельств не смогут сохранить объективность и независимость от правительства США. Например, в случае политического кризиса как ранней стадии перехода к войне власти США могут напрямую – официально или неофициально - приказать ICANN или Verisign осуществить технические операции, чтобы попытаться нарушить связь России с глобальным Интернетом.

На данный момент нет никакой информации о прецедентах, когда NTIA не одобряла запросы ICANN на обновление файла корневой зоны. Также неизвестны прецеденты, когда правительство США со своей стороны требовало, чтобы ICANN внесла какие-либо изменения в процессе обслуживания корневой зоны. Формально контракт об исполнениифункцийи IANA не дает правительству США подобных полномочий. Кроме того, ICANN, IANA, Verisign и РРИ неоднократно подчеркивали, что выполняют четко определенные и стандартизированные технические функции и никогда не будут вовлечены в политические вопросы.

---

[34] ASN – это идентификатор нескольких IP-сетей и роутеров, объединенных под одной системой.

[35] Протоколы, которые управляют обменом маршрутной информацией между автономными системами.

Проблема в том, что безопасность, стабильность и устойчивость национальных сегментов глобальной инфраструктуры Интернета стала важнейшим и чувствительным вопросом национальной безопасности государств, включая такие кибердержавы, как Россия.

Учитывая экономическое влияние зависимого от Интернета бизнеса и другой деятельности на национальную экономику, стабильность и безопасность этой инфраструктуры безусловно входит в число основных национальных интересов государства. Когда ставки настолько высоки, как в сфере стратегической стабильности, решения принимаются исходя не из нынешних намерений партнера, а из основе его потенциальных возможностей. Какими бы безосновательными с точки зрения реальных инцидентов ни казались опасения России по поводу вмешательства правительства США в работу системы УИИ, они имеют под собой определенную логику – логику стратегической стабильности, которая требует, чтобы лицо, принимающее решения, оценивало все возможности, которые потенциальный противник может использовать для нанесения ущерба, независимо от сопутствующего ущерба и собственных издержек. С точки зрения национальной безопасности и стратегической стабильности власти США обладают юридическими возможностями, которые гипотетически могут быть использованы для нарушения доступа России к глобальному Интернету или для изоляции Рунета от глобального Интернета. В случае дальнейшей эскалации политического кризиса – необязательно военного – эти возможности гипотетически могут быть использованы для оказания давления на Россию посредством ограничения ее доступа к Интернету. Именно так, если судить по официальным заявлениям, воспринимаетт ситуацию Совет безопасности России.

Когда ставки настолько высоки, как в сфере стратегической стабильности, решения принимаются исходя не из нынешних намерений партнера, а из основе его потенциальных возможностей.

Поэтому, с точки зрения России, проблема существует. Более того, если ее не решать, в конечном счете это может послужить выбору таких политик, которые спровоцируют фрагментацию Интернета в глобальном масштабе. Такой сценарий затронет не только Россию – из-за распределенной структуры сетей пострадает весь мир.

Какие потенциальные решения могут развеять опасения России, пойти на пользу США и глобальному сообществу? Если отталкиваться от нынешней российской позиции, существуют по меньшей мере два возможных пути.

Первый – повышение прозрачности и подотчетности бизнес-процессов, обеспечивающих функционирование системы УИИ. Этот путь совпадает с заявленными целями процесса передачи ответственного управления функциями IANA. Предлагаемая реформа управления ICANN должна помочь в достижении этих целей. В результате реформы будет создано квазиправительство с управляющим советом, набором внутренних правил, процедурой независимого надзора с обязательными полномочиями, а также ряд организаций поддержки и консультационных комитетов. Управляющие советы должен будет рассматривать рекомендации консультационных органов, но только если достигнут «полный консенсус» по этим рекомендациям.[36] Консерваторы в США и некоторые государства, включая Россию, критикуют реформу из-за того, что национальные правительства будут обладать незначительным весом в новой структуре. Кроме того, пока неясно, как реформа скажется на выполнении конкретных бизнес-процессов.

[36] "We the Networks," p. 2.

Контракт о функциях IANA с правительством США истек 30 сентября 2015 г. Министерство торговли США использовало одну из опций для продления контракта до 30 сентября 2016 г. Дебаты о реформе ICANN продолжились на заседаниях ICANN в июне 2015 г. (Буэнос-Айрес) и в марте 2016 г. (Марракеш).[37] На заседании в Буэнос-Айресе был запущен трехэтапный процесс передачи надзора над IANA. Как отмечалось выше, процесс должен завершиться к осени 2016 г. Согласно ответам, которые получила Координационная группа по передаче координирующей роли в исполнении функций IANA (ICG)от трех сообществ (сообщество Рабочей группы по проектипрованию Интернет (IETF), Сообщество имен и Сообщество номеров) процесс передачи должен охватить основные функции IANA, связанные с глобальной инфраструктурой Интернета, в том числе роль IANA в управлении корневой зоной DNS. Однако реформа не касается общего надзора за другими этапами бизнес-процесса менеджмента корневой зоны DNS. Кроме того, поскольку Verisign как сторона технического обслуживания корневой зоны имеет отдельный контракт с NTIA и не является участником контракта NTIA с ICANN, еего функции могут остаться за рамками процесса передачи надзора над IANA. На конференции ICANN в Буэнос-Айресе ходили слухи, что надзор за техническими функциями Verisign также подвергнется процессу передачи, но официальных подтверждений пока не было.

С точки зрения национальной безопасности и стратегической стабильности власти США обладают юридическими возможностями, которые гипотетически могут быть использованы для нарушения доступа России к глобальному Интернету.

Если процесс повышения прозрачности и подотчетности управления системой УИИ посредством реформирования IANA столкнется с определенными ограничениями и отсрочками, Россия вполне может начать поиск других вариантов.

Одна из возможностей – обеспечение гарантий бенефициарам этих бизнес-процессов. В случае с системой УИИ бенефициарами являются все государства. Поскольку основную озабоченность высказывает Россия, гарантии могут обсуждаться в ограниченном кругу акторов, включая, разумеется Россию и США. Участие других крупных игроков в киберпространстве – Китая и Евросоюза – пойдет на пользу такому механизму гарантий. Гарантии необязательно должны быть очень сложными. Одна согласованная норма послужит полезной основой для дальнейшего консенсуса по данной проблематике – например, под эгидой ГПЭ ООН.

Норма может сводиться к невмешательству правительств в функционирование системы уникальных идентификаторов Интернета (УИИ). Конкретно могут быть прописаны два момента:

a. запрещение спонсируемых государством атак на компоненты инфраструктуры системы УИИ на глобальном уровне (корневые серверы DNS и инфраструктура ресурсов нумерации, операторами которой являются IANA и РРИ)

b. запрещение политически мотивированного вмешательства посредством судебных и административных рычагов в работу IANA, Verisign, РРИи других технических структур, осуществляющих бизнес-процессы, связанные с работой систеыы УИИ. Такой шаготвечал бы интересам России и не противоречил базовым целям правительства США в отношении процесса передачи координирующих функций NTIA.

[37] https://www.icann.org/news/announcement-2016-03-10-en.

Рекомендации и дальнейшие шаги

Суммируя, мы предлагаем шесть рекомендаций для двусторонних договоренностей в сфере кибербезопасности:

a. четкое определение порога кибератак на критически важную инфраструктуру, при превышении которогого атака может повлечь контрудар с применением кибер- или других типов оружия;

b. соглашение по набору информации, которой можно обмениваться в случае кибератаки – например, по аналогии с реагированием на биологическую атаку;

c. запрещение автоматического ответного удара в случае кибератак;

d. запрещение атак на основные элементы Интернет-инфраструктуры другого государства;

e. совместная оценка инфраструктуры управления Интрнетом (операторы системы УИИ, в т.ч. IANA и менеджер корневой зоны DNS) с целью установить и оценить, адекватно ли учитываются интересы и вклад всех участников после реформирования ICANN;

f. широкая международная дискуссия по кибербезопасности за рамками двустороннего взаимодействия России и США. Полезной площадкой может стать Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (UN GGE). Идея ненападения (или в более широком смысле невмешательства) в отношении глобальной и критически важной инфраструктуры Интернета может стать еще одним пунктом в списке не имеющих обязательного характера, добровольных политических норм, предложенных в консенсусном докладе ГПЭ в июне 2015 г. Подобная норма, даже необязательного характера и с широкой формулировкой, будет способствовать международным дипломатическим дебатам по этой тематике благодаря статусу ГПЭ ООН и ее согласованному подходу, которые в значительной степени являются результатом многолетней упорной работы России. Поэтому выработка необязывающей консенсусной нормы в рамках ГПЭ поможет России и США как двум важным участникам деятельности Группы прийти к взаимопониманию и послужит прологом для будущего двустороннего соглашения по поддержанию стабильности, безопасности и отказойустойчивости глобальной инфраструктуры Интернета. При наличии политической воли и понимания значимости этого вопроса работа может начаться уже в 2016 г., когда начнется работа пятого созыва Группы. Однако в долгосрочной перспективе мы считаем актуальным разработать юридически обязывающий международный договор, который будет требовать полного соблюдения норм. Предлагаемые нами двусторонние нормы могут послужить моделью для подобного многостороннего соглашения.

Приложение А: Глоссарий терминов

Как отмечалось в докладе, путь к взаимопониманию между США и Россией по ключевым определениям, связанным с кибер-/информационной безопасностью, был трудным и до сих пор не завершен. Определения некоторых терминов были даны в 2013 г. Группой правительственных экспертов ООН по достижениям в сфере информации и телекоммуникаций в контексте международной безопасности. Однако одна из самых успешных попыток по определению ключевых терминов в этой сфере была предпринята усилиями Института Восток-Запад (США) и Институтом проблем информационной безопасности МГУ (Россия). В 2014 г. эксперты двух институтов опубликовали первые 40 согласованных определений ключевых терминов в сфере кибербезопасности: https://dl.dropboxusercontent.com/u/164629289/terminology2.pdf.

Приведенный ниже глоссарий основан на их списке, с незначительными редакторскими изменениями. Более детальное объяснение, а также другие определения можно найти в докладе, опубликованном двумя институтами.

Критически важная киберинфраструктура – киберинфраструктура, которая необходима для осуществления жизненно важных функций, поддержания общественной безопасности, экономической стабильности, национальной безопасности, международной стабильности, а также для поддержания работоспособности и функций эффективного восстановления критически важного киберпространства. Кибератака – наступательное использование кибероружия с целью нанесения вреда определенной цели и/или нарушения нормального функционирования элементов информационной системы

Киберконфликт – ситуация между двумя или несколькими государствами или организованными группами, при которой враждебные кибератаки приводят к ответным действиям

Кибероборона – организованная совокупность действий для защиты, смягчения воздействия кибератак и эффективного восстановления.

Кибершпионаж – кибероперация по получению несанкционированного доступа к чувствительной информации скрытыми методами.

Кибербезопасность – свойство киберпространства, позволяющее индивидуумам или организациям защищать цифровые активы от взлома или эксплуатирования базовых функций. Включает способность выявлять кибератаки, реагировать на них, восстанавливаться после них и осуществлять сдерживание

Киберпространство – электронная среда, посредством которой информация создаётся, передаётся, принимается, хранится, обрабатывается и уничтожается.

Киберугроза – предполагаемая или выявленная опасность использования киберуязвимости.

Кибервойна – высшая степень киберконфликта между двумя или несколькими государствами, во время которой государственные акторы предпринимают кибератаки против киберинфраструктур противника как часть военной кампании, которая может быть официально объявлена одной из сторон или может проводиться без официального объявления (де-факто).

Боевые действия в киберпространстве – организованная серия кибератак против киберинфраструктуры, которые санкционированы государственными акторами как часть военного конфликта

Кибероружие – программное обеспечение или оборудование, предназначенные для нанесения ущерба в киберпространстве

Информационное пространство – любая среда, в которой информация создается, передается, принимается, хранится, обрабатывается или уничтожается.

Информационная война – высшая степень информационного конфликта между двумя или несколькими государствами, когда информационные операции проводятся государственными акторами для достижения военно-политических целей.

Приложение B: Интернет-инфраструктура

Чтобы понять технологический контекст затронутой темы, необходимо иметь базовое представление о том, что такое глобальная инфраструктура Интернета, как она функционирует, как она контролируется и управляется и, наконец, как теоретически государство может быть отключено от глобального Интернета. Поэтому стоит остановиться на некоторых базовых фактах о системе уникальных идентификаторов Интернета (УИИ).

В децентрализованном глобальном Интернете с присущей ему способностью к масштабированию, распределенной сетевой архитектурой и высокой степенью устойчивости существует только один глобальный централизованный и иерархизированный комплекс инфраструктуры. Это система уникальных идентификаторов, которая является основой и ядром Интернета. Она обеспечивает функционирование Интернета в глобальном масштабе. Без системы УИИ не было бы Интернета как такового, и это единственная система, в отношении которой данное утверждение верно. Она включает в себя три инфраструктурных подсистемы:

- Глобальная система доменных имен (DNS) – набор протоколов и глобальная иерархически распределенная база данных, которые предназначены для преобразования удобных для человека доменных имен в данные в других форматах, включая преобразование доменных имен с адресами IPv4 и IPv6. Однако, как отмечает Общество Интернет, сегодня DNS выполняет гораздо больше функций и служит своеобразной информационно-справочной службой при взаимодействии человека с машиной и машин друг с другом. Помимо IP-адресов DNS используется для поиска почтовых серверов, криптографических ключей, оценки широты и долгыоты и других типов данных. Большинство видов использования Интернета находится в критической зависимости от DNS и SSR ее функционирования. Хотя для функционирования самого Интернета DNS не так важна, эта система жизненно необходима для конечных пользователей и компаний, Однако многие полагают, что очень скоро благодаря усовершенствованным поисковым системам DNS станет ненужной.

- Система распределения номерных ресурсов в Интернете, которая состоит из системы распределения IP-адресов и системы раздачи номеров в автономных системах.

- Система IP-адресов является основным компонентом глобальной инфраструктуры Интернета. Как гласит RFC 770 (январь 1980 г.) IP-адрес – это «числовой ярлык, присваиваемый каждому устройству (например, компьютеру, принтеру), участвующему в компьютерной сети, которая использует для коммуникации Интернет-протокол». Две основные функции IP – идентификация интерфейса хоста или сети и обращение к их местонахождению. Уникальность адресов Интернет-протокола (IP) является фундаментальным технологическим требованием для обеспечения коммуникации и передачи трафика между сетями в Интернете. Уникальность IP гарантирует, что пакеты данных в конечном итоге достигнут адресата, где бы он ни находился. Если IP-адрес не будет соответствовать каким-то критериям уникальности – например, если разные узлы сети используют одинаковые IP, – произойдет сбой в системе маршрутизации, которое приведет к нарушению доступа к отдельным или ко всем узлам сети.

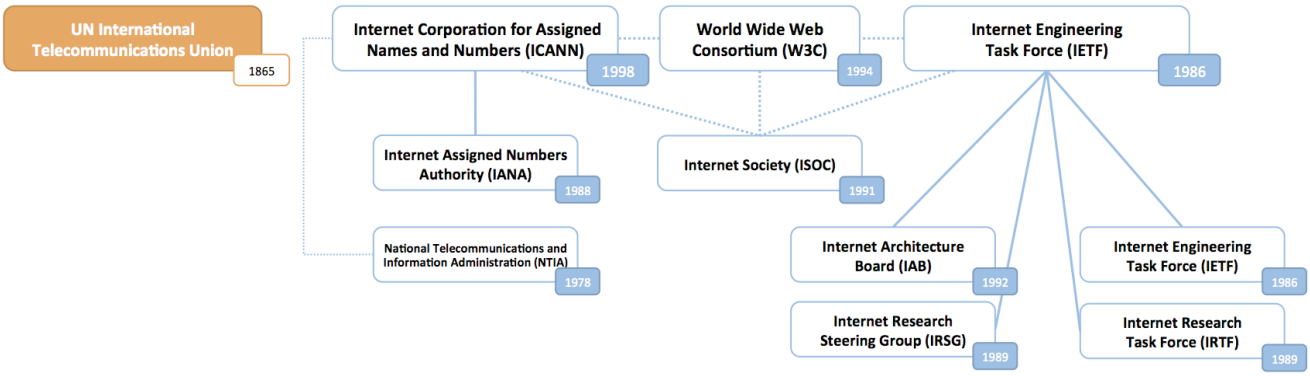
- Автономные системы (АС) и номера Автономных Систем. Автономная система – это совокупность сетей под единой административной политикой маршрутизации. Концепция AS появилась как своего рода надстройка над IP-уровнем, которая позволяет агрегировать миллиарды IP в ограниченные и управляемые, но по-прежнему уникальные группы. Необходимость подобной агрегации обусловлена предельными возможностями системы междоменной маршрутизации. В настоящее время система преимущественно использует протокол BGP-4 для построения маршрутов между АС, общее число которы-х составляет около 75 000. Количество маршрутов, доступных напрямую или опосредованно, зависит от общего числа доступных АС. Это важно для процесса расчета путей маршрутизации, который выполняется на сетевом оборудовании, использующем BGP. Количество доступных маршрутов и их комбинаций в Интернете определяет размер так называемых таблиц маршрутизации, которые расчитывают маршрутизаторы. Поэтому без агрегации междоменной маршрутизации до уровня АС маршрутизация осуществлялась бы путем отправки пакетов данных напрямую между узлами сети с разными IP. Даже для IPv4 с его глобальным пулом всего из 4,25 млрд уникальных адресов таблицы маршрутизации были бы неоправданно огромными, а процесс расчета путей маршрутизации – чрезвычайно ресурсозатратным. Что касается IPv6 с его глобальным пулом из 2^{128} уникальных адресов, то глобальная маршрутизация в Интернете стала бы невозможной из-за ограниченных вычислительных мощностей маршрутизаторов. Таким образом, по сути АС – это необходимое средство упрощения маршрутизации в Интернете.

Таким образом, вместе с номерами Автономных Систем, DNS и глобальной системой маршрутизации ресурсы IP-адресов составляют систему уникальных идентификаторов Интернета, которая первоначально была описана в RFC 791: «Имя обозначает, что мы ищем. Адрес обозначает, где это находится. Маршрут показывает, как туда попасть».

- Наконец, существуют параметры Интернет-протоколов и номера портов этих протоколов. Параметры протоколов и номера портов, которые используются для межсетевой коммуникации в Интернете, – это предписанные характеристики, представляющие собой третий, последний компонент системы УИИ. Скоординированное использование номеров порта многочисленными операторами сети не требует такой мощной глобальной системы серверов, как DNS. На самом деле параметры протоколов и номера порта – это открытая база данных, которую ведет ответственная структура, но они доступны для всех сетевых операторов в Интернете.

Физическая инфраструктура присутствует только в DNS и системе распределения ресуров нумерации. Интернет-протоколы и их порты не являются физическими объектами; это стандарты, обеспечивающие взаимодействие сетей в глобальном Интернете. Подорвать их инфраструктуру невозможно, потому что она как таковая не существует.

Приложение C: Схема организации управления Интернетом



Об авторах

Олег Демидов – консультант ПИР-Центра, ведущего российского неправит ельственногоисследовательского центра в сфере глобальной безопасности, и член Экспертного совета ПИР-Центра. Выпускник Международной школы по вопросам глобальной безопасности ПИР-Центра (2012). С 2014 года Олег является экспертом Когсультативной исследовательской сети (RAN) при Глобальной комиссии по управлению Интернетом (GCIG). Он также является членом Комитета по вопросам управления Интернетом в рамках Координационного центра доменов .RU/.РФ. К сфере его экспертизы относятся: глобальное управление киберпространством и Интернетом, управление инфраструктурой Интернета и защита критической ИКТ-инфраструктуры. С 2011 года Олег участвует в обсуждении этих тем в рамках встреч Корпорации Интернета (ICANN), всемирного Форума по управлению Интернетом (IGF), саммита NETmundial, EuroDIG, РИГФ, АТССБ, экспертных консультаций ЮНИДИР.

Виталий Каберник – ведущий научный сотрудник Центра стратегических исследований МГИМО. Член и эксперт Рабочей группы ПИР-Центра по кибербезопасности и управлению Интернетом. Виталий является автором многочисленных публикаций по теме трансформации военных доктрин, связанных с появлением новых концепций, таких как революции в военной сфере, кибервойны, гибридные конфликты и так далее. К сфере его экспертизы относятся: вопросы нераспространения, публичная дипломатия, стратегическая разведка, психологические операции, кибероружие, алгоритмы шифрования и защита критической IT-инфраструктуры.

Елена Черненко – руководитель отдела внешней политики газеты «Коммерсантъ» (Москва) и член пресс-пула МИД России. В сферу ее интересов входит кибербезопасность, российская внешняя политика, отношения России с Западом и странами на постсоветском пространстве. Является участником программы молодых лидеров Мюнхенской конференции по безопасности-2015, членом Ссовета ПИР-Центра, членом Совета по внешней и оборонной политике и членом Рабочей группы по будущему российско-американских отношений.

Томас Ремингтон – профессор политологии в Университете Эмори. Также является ведущим научным сотрудником Международного центра изучения институтов и развития Высшей школы экономики в Москве и сотрудником Центра Дэвиса по изучению России и Восточной Европы в Гарвардском университете. Получил степень доктора политических наук в Йельском университете в 1978 г. и степень магистра в области изучения России и Восточной Европы в Йеле в 1974 г. Автор ряда книг и статей о России и посткоммунистической политике. Среди его публикаций: *Presidential Decrees in Russia: A Comparative Perspective* (Cambridge University Press, 2014); *The Politics of Inequality in Russia* (Cambridge University Press, 2011); *The Russian Parliament: Institutional Evolution in a Transitional Regime, 1989–1999* (Yale University Press, 2001); и *The Politics of Institutional Choice: Formation of the Russian State Duma* (в соавторстве со Стивеном С. Смитом) (Princeton University Press, 2001). Среди его книг: *Politics in Russia* (7th edition, Longman, 2011); *Parliaments in Transition* (Westview Press, 1994); и *The Truth of Authority: Ideology and Communication in the Soviet Union* (University of Pittsburgh Press, 1988). В настоящее время занимается изучением неравенства и социальной политики в России и Китае.

Крис Спирито – консультант по ядерной и кибербезопасности в Национальной лаборатории Айдахо при Министерстве энергетики США. Занимается вопросами защиты объектов ключевой инфраструктуры от кибератак и разработкой моделей для обучения и подготовки специалистов по системной безопасности. До прихода в Национальную лабораторию Айдахо Крис работал в Центре инжиниринга национальной безопасности в корпорации MITRE. Крис начал работу в группе информационной борьбы MITRE в 1998 г., большую часть своей карьеры он занимался поддержкой инициатив по кибербезопасности в Министерстве обороны и спецслужбах. В сферу интересов Криса в MITRE входили точки соприкосновения кибер- и ядерной безопасности, киберанализ на иностранных языках, киберобучение, разработка международных кибернорм и мер укрепления доверия. Крис является приглашенным лектором факультета права Университета Тарту и одним из авторов книги, выпущенной Международным институтом стратегических исследований *Evolution of the Cyber Domain: The Implications for National and Global Security.*

Рабочая группа по будущему российско-американских отношений

Российские участники

Павел Андреев, Исполнительный директор, РИА Новости

Олег Барабанов, Заведующий кафедрой и профессор, МГИМО; профессор факультета мировой экономики и мировой политики НИУ ВШЭ

Тимофей Бордачёв, Директор Центра комплексных европейских и международных исследований, факультет мировой экономики и мировой политики НИУ ВШЭ; руководитель исследовательских программ, Совет по внешней и оборонной политике

Сергей Веселовский, Доцент кафедры мировых политических процессов МГИМО

Александр Габуев, Старший научный сотрудник, руководитель программы "Россия и АТР", Московский Центр Карнеги

Олег Демидов, консультант, ПИР-Центр

Игорь Зевелев, Директор, московский офис Фонда МакАртуров

Виталий Каберник, Ведущий эксперт, Центр военно-политических исследований МГИМО; член Рабочей группы по кибербезопасности, ПИР-Центр

Сергей Караганов, Декан факультета мировой экономики и мировой политики НИУ ВШЭ; почетный председатель Президиума, Совет по внешней и оборонной политике

Василий Кашин, Научный сотрудник, Центр анализа стратегий и технологий

Екатерина Колдунова, Заместитель декана факультета политологии, доцент кафедры Востоковедения МГИМО

Валерий Конышев, Профессор кафедры теории и истории международных отношений СПбГУ

Василий Кузнецов, доцент Московского государственного университета, Директор, Центр политических систем и культур

Федор Лукьянов, Главный редактор, «Россия в глобальной политике»; председатель Президиума, Совет по внешней и оборонной политике

Борис Межуев, Доцент, Московский государственный университет; соредактор портала Terra America

Геворг Мирзаян, Научный сотрудник, Институт США и Канады, Российская Академия наук

Наталья Стапран, Доцент кафедры Востоковедения МГИМО

Дмитрий Суслов, Заместитель директора, Центр комплексных европейских и международных исследований НИУ-ВШЭ; Заместитель директора по исследованиям СВОП

Андрей Сушенцов, Доцент кафедры прикладного анализа международных проблем, МГИМО

Михаил Троицкий, Доцент кафедры международных отношений и внешней политики Россиб, МГИМО

Елена Черненко, специальный корреспондент, ИД "Коммерсантъ"

Американские участники

Рави Абделал, Профессор бизнес-администрирования, Гарвардская школа бизнеса; директор Центра российских и евразийских исследований им. Дейвиса, Гарвардский университет

Александра Вакру, Исполнительный директор Центра российских и евразийских исследований им. Дейвиса, Гарвардский университет

Кит Дарден, Доцент, Школа внешнеполитической службы, Американский университет

Тимоти Колтон, Профессор государственного управления и российских исследований, декан Департамента политических исследований, Гарвардский университет

Александр Кули, Директор, Институт Гарримана, профессор политических наук, колледж Барнарда, Колумбийский университет

Паулин Джонс Луонг, Профессор политических наук и директор Международного Института Университета Мичигана

Джеффри Манкофф, Заместитель директора и научный сотрудник, Программа России и Евразии, Центр стратегических и международных исследований

Кевин Райан, Директор проекта по оборонным исследованиям и разведке, Центр международных исследований им. Белфера, Гарвардский университет

Томас Ремингтон, Профессор политических наук, Университет Эмори

Рэндалл Стоун, Профессор политических наук, Директор центра польских и центральноевропейских исследований и Центра по конфликтам и сотрудничеству им. Питера Д. Уатсона, Университет Рочестера

Кори Уэлт, Заместитель директора, Институт европейских, российских и евразийских исследований, Школа международных дел им. Элиота, Университет им. Джорджа Вашингтона

Генри Хейл, Профессор политических наук и международных отношений, Университет им. Джорджа Вашингтона

Сара Хюммель, доцент департамента политических наук, университет Иллинойс в Урбана-Шампэйн

Сэмюэл Чарап, Старший научный сотрудник по России и Евразии, Международный институт стратегических исследований – США

Йошико Эррера, Профессор политических наук, Университет Висконсина, Мэдисон

Рабочая группа по будущему российско-американских отношений предлагает перспективным специалистам из ведущих американских и российских исследовательских центров и университетов поделиться своим видением решения самых острых проблем двусторонних отношений. Мы содействуем обмену мнениями и открытым дискуссиям среди ученых нового поколения. Мы нацелены на творческий анализ проблем и выработку политических рекомендаций, отражающих общность взглядов России и США по многим вопросам, которая, тем не менее, часто подавляется взаимным недоверием. Мы полагаем, что наш подход, основанный на двустороннем диалоге, дает наилучшие возможности улучшить взаимопонимание и разрешить спорные проблемы между нашими странами.

WORKING GROUP ON THE FUTURE OF U.S.- RUSSIA RELATIONS

РАБОЧАЯ ГРУППА ПО БУДУЩЕМУ РОССИЙСКО-АМЕРИКАНСКИХ ОТНОШЕНИЙ