Общая основа: отношения США и НАТО с Россией в киберпространстве

Геофф ван Еппс[*]

Введение

За последние два десятилетия в глобальной стратегической картине произошли существенные изменения, в число которых входят падение Железного занавеса и распад Советского Союза, ускоренная глобализация, более широкое использование цифровых информационных технологий во всех аспектах жизни, подъем Китая и Индии, глобальные финансовые кризисы, политические революции Арабской весны и появление насильственного исламистского экстремизма в качестве основной характерной особенности геополитического пейзажа. И в то же время, уже двадцать лет многие ключевые характеристики динамики на международной арене остаются неизменными, в том числе непостоянство ситуации и нестабильность на Ближнем Востоке, отсутствие развития на большей части африканского континента, постоянно усиливающаяся интеграция глобальной экономики, огромное превосходство Соединенных Штатов в качестве глобального актора в мировых делах и ключевая роль, которую играют такие другие государства как Объединенное Королевство, Германия и Россия.

Среди всего того, что изменилось и того, что осталось неизменным, немногое можно рассматривать изолированно. Наоборот, комплексный и взаимосвязанный характер сегодняшней международной системы требует анализа, который учитывает отношения между акторами и проблемами и рассматривает множество последствий, которое их взаимодействие неизбежно порождает. Две ключевые особенности текущей стратегической среды – как раз те две, которые находятся в фокусе этой статьи, – это незаменимость информационных технологий во всех аспектах современной жизни и остающееся все таким же важным значение России в качестве актора на мировой сцене.

Движимая растущей зависимостью современного общества от цифровой технологии и уязвимостью цифровых систем от кибернетических угроз, кибербезопасность появилась как критически важный аспект национальной безопасности, породив быстро растущую индустрию, которая занимается техническими, правовыми и политическими вызовами наших дней. В то же время, Соединенные Штаты и Организация Североатлантического Договора (НАТО), соперничают с Российской Федерацией, которая больше не представляет собой угрозы для их существования, но все еще располагает достаточной мощью для того, чтобы требовать

---

[*] Геофф ван Еппс – подполковник армии США. Эта статья основывается на исследовании, проведенном автором в период его работы в качестве старшего сотрудника Европейского центра исследований по вопросам безопасности им. Джорджа С. Маршалла в Гармише, Германия, в 2012-2013 годах.

неусыпного внимания и для того, чтобы играть роль препятствия во многих важных глобальных проблемах. США и НАТО неоднократно и публично заявляли, что улучшение отношений и усиление сотрудничества с Россией являются основным приоритетом, но риторика редко находила выражение в конкретных улучшениях отношений или в существенном прогрессе по критическим темам, находящимся на повестке дня. Однако, кибербезопасность является областью стратегического значения, в которой реальный прогресс возможен. Символическим первым шагом в этом направлении является объявленная в июне 2013 года двусторонняя договоренность о совместной работе в области кибербезопасности, хотя охват соглашения скромный и оно может служить только исходным пунктом для долгосрочной и более обширной программы сотрудничества. Более существенное улучшение отношений США и НАТО с Россией является жизненно важным, имея в виду взаимосвязанность всех трех акторов и их статус трех наиболее важных акторов в делах безопасности современной Европы, – и в определенной степени – глобальной безопасности. Ввиду существенных кибернетических возможностей России (и продемонстрированное ею желание использовать их), ее долгосрочного стремления получить признание в качестве лидера в мировых делах и требования общественности разработать международные нормы поведения в киберпространстве, кибербезопасность является первостепенной темой в отношениях США и НАТО с Россией.

Комплексная взаимозависимость и киберпространство

Активное взаимодействие Соединенных Штатов с Россией неизбежно, так как оба государства являются одними из немногих государств с глобальными интересами и потенциалом продвигать эти интересы. НАТО неразрывно связано с США, с которыми у них множество общих ценностей и целей, тогда как географическая близость к России и переплетающиеся (а иногда и находящиеся в противоречии) интересы в области безопасности делают постоянное взаимодействие с Российской Федерацией неизбежным и очень важным.

Следовательно, увеличивающаяся взаимозависимость между США и НАТО с одной стороны, и Россией с другой, не является неожиданным. Благодаря ускорению глобализации и развитию технологий, за последние двадцать лет расходы на транспорт и коммуникации резко падают, существенно уменьшая влияния удаленности на экономические, военные, социальные и другие стороны взаимодействия между государствами, организациями и даже отдельными людьми.[1] Уменьшающиеся цены привели к увеличению объема взаимодействий между акторами, предоставляя дополнительные выгоды всем участвующим сторонам, и создали ситуацию, в которой каждый из игроков в сети взаимоотношений поддерживает опреде-

[1] Joseph S. Nye, *Understanding International Conflicts*, 4th ed. (New York: Longman, 2003), 185–92.

ленную степень взаимозависимости с другими.[2] Эта взаимозависимость – определяемая как взаимная зависимость сторонами, или способность этих сторон оказывать реципрокное влияние друг на друга – является отличительной чертой глобализации и определяющим фактором в современной международной системе.[3]

Идея, что акторы в международной системе находятся во взаимосвязанных отношениях и таким образом зависят друг от друга, что эта зависимость охватывает почти все измерения их отношений и что она оказывает влияние на поведение акторов, является одновременно и простой, и сильной. За последние три десятилетия эта теория приобрела множество сторонников и была широко воспринята, выдвигаясь в середину течения международного политического мышления и оказывая влияние на развитие внешней политики Соединенных Штатов и многих других стран, в особенности развитых индустриальных и постиндустриальных демократий. Применение представления о комплексной взаимозависимости к мировым делам имело рекурсивное влияние на международную систему, одновременно определяя, как международные акторы рассматривают свои отношения, как формируют свою политику и как выбирают линию поведения, в то же время предлагая приемлемые объяснения тому, как и почему такое поведение становится причиной того развития событий, которое имеет место на международной арене. Наряду с этим, идеалистический подход к взаимозависимости – в частности комплексной взаимозависимости, с ее глубокими отношениями во множестве измерениях – ведет к вроде бы неизбежному уменьшению числа международных конфликтов из-за расширения ограничений на воинственное поведение, способствуя созданию ощущения общности среди глобальных акторов и уменьшая поводы для конфликтов.[4] Но хотя комплексная взаимозависимость выросла по значению и степени приятия, она не оправдала надежды на укрепление глобального мира и сотрудничества.[5] В целом причина в том, что отношения взаимозависимости углубляют и укрепляют связи между акторами, но такие взаимозависимости все еще могут приводить к соперничеству и даже конфликтам. Главное, даже в ситуациях, которые не являются играми с нулевой суммой, существуют асимметрии, и распределение выгод между участвующими акторами неравномерно. В итоге, вза-

---

[2] Robert O. Keohane and Joseph S. Nye, *Power and Interdependence*, 3rd ed. (New York: Longman, 2001), 7–9.

[3] Joseph S. Nye, "Independence and Interdependence," in Nye, *Power in the Global Information Age* (New York: Routledge, 2004), 154; Keohane and Nye, *Power and Interdependence*, 7.

[4] Традицию убежденности, что взаимозависимость станет концом войн можно проследить до времени перед Первой мировой войной в таких работах как Norman Angell, *The Great Illusion: A Study of the Relation of Military Power in Nations to Their Economic and Social Advantage* (New York: Putnam, 1910). Одним из анализов влияния взаимозависимости на межгосударственные конфликты в период после Холодной войны является работа Susan M. McMillan, "Interdependence and Conflict," *Mershon International Studies Review* 41 (1997): 35–36.

[5] Nye, *Understanding International Conflicts*, 195.

имозависимость не означает регулярное сотрудничество и конец конфликтам. Наоборот, она создает условия, которые одновременно способствуют более широкому сотрудничеству в некоторых областях, тогда как в других порождает конфликты.[6]

Киберпространство дает нам ясную иллюстрацию ситуации, в которой акторы участвуют одновременно как в сотрудничестве, так и в жесткой конкуренции, часто между одними и теми же акторами и часто в одно и то же время. Быстрое развитие и распространение передовых информационных технологий за последние десятилетия создали киберизмерение комплексной взаимозависимости, которое имеет свои уникальные особенности. Эта информационная революция привела к радикальным изменениям в политике, бизнесе, культуре и других областях жизни общества, способствуя росту организаций как сетей, создавая потребность в новых ролях управления, в целом бросая вызов иерархической бюрократии и порождая тенденцию к децентрализации.[7] Последствия этих изменений трудно преувеличить. Бюрократию, и государственную и корпоративную, постоянно обходят формальные и неформальные организации, которые более быстро и эффективно передают и обрабатывают информацию, оказывающую влияние на большие группы людей быстрее, чем традиционные институции. Отдельные люди и частные организации присоединились к государствам в качестве прямых игроков в мировой политике. Произошло то, что на фасаде ненарушимого и незыблемого суверенитета государств появились признаки изменений, по мере того как транснациональные коммуникации стали давать широким массам возможность принимать участие в решении проблем, которые в прошлом были прерогативой единственно государств.[8] Эти изменения не происходят равномерно по всему миру – их появление было гораздо более интенсивным в «зоне демократического мира», и они практически отсутствовали в неразвитых регионах. Но, тем не менее, они представляют собой огромный сдвиг в осуществлении контактов между разными обществами и показывают наличие потенциала для еще более обширных изменений статус-кво.[9]

В то же время как они спровоцировали такие драматические социальные изменения, многие из этих усовершенствований только усилили проявления особенности комплексной взаимозависимости: появление сильных негосударственных глобальных акторов; важность таких не связанных с военной безопасностью проблем как экономика и окружающая среда; и влияние на решения о применении силы в эпоху средств массовой информации, активистов и социальных сетей. Компьютерные сети, которые сделали возможным осуществление многих из этих перемен – киберпространство – позволяют международным акторам «охватывать» друг друга посредством цифровой связи со скоростью, легкостью и частотой, невоз-

---

6 Nye, “Independence and Interdependence,” 154.

7 Nye, “The Information Revolution and American Soft Power” (2001), в Nye, *Power in the Global Information Age* (New York: Routledge, 2004), 81–82.

8 Там же, 83–88.

9 Keohane and Nye, *Power and Interdependence*, 217–18.

можными прежде.[10] Разумеется, сущность киберпространства – это его связанность, и так как международные цифровые транзакции в обозримом будущем будут продолжать расти, связи, которые соединяют акторов в международной системе, будут становиться все более прочными, и их взаимозависимость будет увеличиваться.[11] В то же время, уникальный характер киберпространства, его относительная незрелость в качестве среды и отсутствие повсеместно принятых норм поведения в нем станут новыми вызовами, которые будут влиять на эти отношения и потенциально могут изменить динамику комплексной взаимозависимости новыми и непредсказуемыми способами.

Киберпространство и кибербезопасность

Цифровая взаимосвязанность стала повсеместной чертой современной жизни и как причина, и как результат расширяющейся взаимозависимости, которая является определяющей для международной системы. Информационная технология пронизывает и делает возможным каждый аспект жизни общества. Эксплозивный рост связанности компьютеров и компьютерного оборудования в сетях, который позволяет быструю коммуникацию огромных объемов информации при устойчиво уменьшающихся ценах, стал причиной таких глубоких изменений, что развитие и интегрирование этих технологий воспринимается как сравнимое по масштабу и последствиям с Промышленной революцией.[12] Цифровые технологии лежат в основе функционирования нашего мира, предоставляя средства для глобальной коммуникации, позволяя продавать и покупать товары и услуги, осуществлять финансовые транзакции, управлять воздушным движением, предсказывать погоду, эксплуатировать критическую инфраструктуру, управлять производственными системами, руководить операциями военных формирований, и выполнять тысячи других жизненно важных функций с беспрецедентной скоростью и точностью. Развитие этих технологий привело к огромным выгодам в мировом масштабе, но оно происходит не без сопутствующих проблем. Наиболее значимый из них – это кибербезопасность, которая охватывает набор связанных технических, политических и правовых вопросов, которые в совокупности могут угрожать положительному конечному результату функционирования нынешних сетей глобальной взаи-

---

[10] Will Goodman, “Cyber Deterrence: Tougher in Theory than in Practice?” *Strategic Studies Quarterly* 4:3 (Fall 2010): 102-35, цитата на с. 121.

[11] Международный Союз Телекоммуникаций, *Измерение информационного общества 2012* (Женева: Международный Союз Телекоммуникаций), ежегодный доклад специального агентства ООН, в котором делается попытка оценить количественно широту и глубину распространения информационных и коммуникационных технологий в мировом масштабе.

[12] Nye, *Understanding International Conflicts,* 215.

мозависимости и таким образом изменить саму основу многих текущих, ключевых отношений в международной системе.[13]

Информационно-технологические сети, которые в совокупности – аппаратные средства, программное обеспечение, линии связи и данные, из которых они состоят, – способствуют нашей цифровой взаимосвязанности, стали известны как киберпространство, комплексная и постоянно меняющаяся среда, являющаяся частично физической и частично виртуальной.[14] Ее уникальный характер делает концептуализацию киберпространства серьезным вызовом, и консенсус относительно точной дефиниции киберпространства пока не был достигнут.[15] Большинство определений, однако, совпадают с описанием, используемым в вооруженных силах США: «глобальный домен в информационной среде, включающий взаимозависимые элементы инфраструктуры информационно-технологической сети, в том числе Интернет, телекоммуникационные сети, компьютерные системы и встроенные процессоры и контроллеры».[16] Однако, отсутствие согласия о том, что представляет собой киберпространство, остается большой проблемой, так как оно оказывает влияние на то, как акторы рассматривают эту среду и развивают соответствующие способности, формируют политику и, в конечном итоге, действуют по вопросам киберпространства.[17]

Трудности в определении киберпространства неизбежно приводят к спорам по ключевым концепциям, чье окончательное решение оказало бы сильное влияние на последующее мышление по кибервопросам. Важным примером является встроенная в определении киберпространства Вооруженных сил США идея, что киберпространство является пятой сферой военных операций (наряду с сушей, морем, небом и Космосом), из которой проистекают последствия для политики и доктрин, которые могут осложнить дискуссии с союзниками, противниками и даже другими заинтересованными государственными ведомствам, по вопросам кибербезопасности. Министерство обороны США совершило концептуальный скачок, определив киберпространство в качестве сферы операций как «организующая концепция для миссий министерства обороны по обеспечению национальной без-

---

[13] James C. Mulvenon and Gregory J. Rattray, "Addressing Cyber Instability: Executive Summary," *Cyber Conflict Studies Association Web Site* (9 July 2012), 1; доступно на www.thecre.com/fnews/wp-content/uploads/2012/07/CCSA-Addressing-Cyber-Instability.pdf.

[14] Nye, *Cyber Power* (Cambridge, MA: Belfer Center for Science and International Affairs, 2010), 4.

[15] Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz (Washington, D.C.: National Defense University Press, 2009), 24. Сводку дефиниций терминов США, Объединенного Королевства, Канады и Австралии можно найти в David J. Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power* (New York: Routledge, 2011), 36.

[16] United States Department of Defense, *Dictionary of Military and Associated Terms,* Joint Publication 1-02 (Washington, D.C.: Government Printing Office, 2011), 77.

[17] Betz and Stevens, *Cyberspace and the State*, 36-37.

опасности» с тем, чтобы «полностью использовать преимущества потенциала киберпространства».[18] Эта декларация не решает полностью теоретический спор в Министерстве обороны; наоборот, она просто обеспечивает общую концептуальную рамку для обсуждения связанных с кибертематикой проблем и служит больше отправной точкой для дискуссий, чем конечным пунктом мышления о киберпространстве.[19] В то же время теория или политика, разрабатываемые с этой точки зрения, менее ценны, чем попытка гармонизировать действия с другими акторами, которые не рассматривают киберпространство с использованием того же понятийного аппарата.

Может быть, лучшей моделью для визуализации самих систем информационных сетей является модель, предложенная ученым из корпорации RAND Мартином Либицким, который описывает киберпространство как состоящее из трех слоев. Первый слой, который служит скелетом других двух слоев, это физические компоненты, включающие «ящики и (иногда) провода», которые формируют аппаратную часть информационной системы. Средний слой – это синтактический слой, содержащий программное обеспечение с инструкциями и протоколами, которые позволяют средствам аппаратной части функционировать и коммуникировать друг с другом. Верхний слой – это семантический слой, содержащий информацию системы, и следовательно, причину, по которой существует эта система.[20] Модель Либицкого помогает структурировать дискуссии о киберпространстве приданием формы, масштаба и осязаемости этой концепции, но как и все модели имеет свои ограничения и может не выдержать проверку временем, так как сложность информационных систем продолжает увеличиваться, а новые технологии меняют дизайн и функционирование этих систем.

Другой важный продолжающийся спор идет вокруг вопроса, является ли киберпространство международным общим достоянием. Те, кто утверждает, что киберпространство является общим достоянием, основываются на том, что у него есть общие характеристики с такими глобальными объектами общего достояния как воздух, море и Космос, и что идея глобального общего достояния широко принята и понятна для широких кругов. Наиболее значительный вклад идеи киберпространства как объекта общего достояния состоит в том, что, по определению, предметы общего достояния не попадают под юрисдикцию отдельной страны и их совместное использование регламентируется международными нормами – каким как раз и является сегодня, по мнению многих авторитетов, случай с

---

[18] United States Department of Defense, *Strategy for Operating in Cyberspace* (Washington, DC: Government Printing Office, 2011), 5.

[19] Franklin D. Kramer, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework," in *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz (Washington, D.C.: National Defense University Press, 2009), 12. Смотри так же Rattray, "An Environmental Approach to Understanding Cyberpower," in *Cyberpower and National Security,* for a more extensive analysis.

[20] Martin Libicki, *Cyberdeterrence and Cyberwarfare* (Santa Monica, CA: RAND, 2009), 12–13.

киберпространством.[21] Те из экспертов, кто отрицает идею киберпространства как объекта общего достояния, считают, что у идеи того, что у Интернета нет границ и национальные государства не располагают никакой возможностью упражнять суверенитет в киберпространстве, есть недостатки. С их точки зрения, почти вся инфраструктура, составляющая киберпространство – физический слой, если использовать конструкт Липицкого – находится внутри границ суверенных государств, и следовательно, является объектом применения законов этих государств.[22] Разрешение этого спора окажет влияние на дальнейшее развитие киберпространства, его архитектуры, управления и ценностей, которые его формируют.[23] А пока разногласия по этому фундаментальному представлению сдерживают прогресс к достижению международного консенсуса о правилах оперирования в киберпространстве и о том, кто несет ответственность за применение этих правил.

Недостаточная безопасность

Как бы ни воспринимали мы киберпространство, быстрое распространение и более широкое использование информационных технологий во многих случаях опережают способность государств регулировать их использование или даже понимать проблемы, которые новые технологии порождают. Споры о том, как дефинировать киберпространство, думать или нет о нем как о сфере операций, и является ли оно предметом общего достояния, важны, но абстрактны. С другой стороны, факт, что большая часть инфраструктуры того, что сегодня превратилось в киберпространство, была создана с помощью технологий, разработанных без учета потребностей безопасности, делает задачу обеспечения безопасности киберпространства почти сизифовым трудом. Первые проектировщики Интернета были исследователями в четырех университетах в Западных Соединенных Штатах, которые использовали финансирование со стороны федерального правительства в 1960-х, чтобы разработать сеть, позволяющую компьютерам в их институтах коммуникировать напрямую друг с другом. Связь была спроектирована в децентрализованной манере так, чтобы в большей степени способствовать масштабируемости, конфиденциальности и удобстве коммуникации, чем обеспечению безопасности. Его изобретатели думали, что речь идет об установлении связи между тысячами добронамеренных преподавателей и ученых с целью обмениваться результа-

---

[21] Leon E. Panetta, "America's Pacific Rebalance," *Project Syndicate* (31 December 2012); доступно на http://www.project-syndicate.org/commentary/renewing-the-us-commitment-to-the-asia-pacific-region-by-leon-e--panetta. Смотри еще James C. Stavridis and Elton C. Parker, III, "Sailing the Cyber Sea," *Joint Forces Quarterly* 65 (2012): 62; и Mark Barrett, Dick Bedford, Elizabeth Skinner, and Eva Vergles, *Assured Access to the Global Commons* (Norfolk, VA: Supreme Allied Command Transformation, North Atlantic Treaty Organization, 2011), xii–xiii.

[22] James Lewis, "Rethinking Cyber Security—A Comprehensive Approach," speech to the Sasakawa Peace Foundation, Tokyo, Japan (12 September 2011); доступно на http://csis.org/files/publication/110920_Japan_speech_2011.pdf. See also Nye, *Cyber Power*, 15.

[23] Lewis, "Rethinking Cyber Security."

тами исследований, – а не о тех миллиардах машин и пользователей, реализующих жизненно важные и иногда зловещие функции жизни сегодняшнего дня.[24]

По мере того как Интернет взрослел, разрастался и распространялся от академических сред к государственным органам и широкому гражданскому использованию, базовый факт, что технологические строительные блоки Интернета были спроектированы без учета требований безопасности, становился центральной технической проблемой. Сегодня, по словам одного эксперта, «связанность в текущий момент намного обгоняет безопасность».[25] Открытость и легкость использования неизбежно привлекли злоумышленных акторов, чья изощренность и амбиции росли вместе с Интернетом, развиваясь от легких повреждений вебстраниц в 1990-х до хорошо организованных преступных синдикатов, осуществляющих киберпреступления, и руководимых государством программ шпионажа и кибератак в наши дни.[26] США знают об этой уязвимости, и президент Обама в 2009 году в одной из своих речей описал «большую иронию нашей Информационной Эпохи – те технологии, которые дают нам возможность создавать и строить, дают возможность и тем, кто хочет разрушать и уничтожать.[27] Поэтому еще в начале президентского срока администрация Обамы провела пересмотр политики по киберпространству и расширила Комплексную инициативу по национальной кибербезопасности с тем, чтобы противостоять «одному из наиболее серьезных экономических вызовов и вызовов национальной безопасности, с которым мы сталкиваемся как нация».[28]

Партнеры и союзники США также признают серьезность киберугроз и работают для решения этой проблемы. В *Стратегической концепции* НАТО от 2009 года в описании среды безопасности отмечено, что «Кибератаки становятся все более частым явлением, все лучше организованы и причиняют все более дорогостоящий ущерб государственной администрации, бизнесу, экономике и потенциально транспортной инфраструктуре, инфраструктуре поставок и другой критической инфраструктуре; они могут достигать уровня серьезности, который угрожает

[24] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Harper Collins, 2010), 81-83.

[25] Kenneth Geers, *Strategic Cyber Security* (Tallinn, Estonia: Cooperative Cyber Defence Center of Excellence, 2011), 10.

[26] Mulvenon and Rattray, "Addressing Cyber Instability," 1–2.

[27] Barack Obama, "Remarks by the President on Securing our Nation's Cyber Infrastructure," 29 May 2009; доступно на www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

[28] Office of the President of the United States, *Comprehensive National Cybersecurity Initiative* (Washington, D.C.: The White House, 2009), 1; доступно на http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf.

национальному и евроатлантическому процветанию, безопасности и стабильности».[29]

Подобным образом Россия и Китай так же выразили свою озабоченность угрозой, которую представляет собой неадекватная кибербезопасность, наиболее публично в меморандуме, который они внесли в Генеральную ассамблею ООН в 2011 году совместно с Таджикистаном и Узбекистаном, призывающем к созданию международного кодекса поведения для обеспечения информационной безопасности. Их предложение описывало «необходимость предотвратить потенциальное использование информационных и коммуникационных технологий для целей, которые несовместимы с поддержанием международной стабильности и безопасности».[30] Эта тема также имела отзвук в Концепции внешней политики России от 2013 года, которая предлагает создать под эгидой ООН международный кодекс поведения, обеспечивающий информационную безопасность, и который декларирует готовность противодействовать действиям, «чьи цели противоречат международному праву, в том числе и действиям, направленным на вмешательство во внутренние дела и являющимися угрозой международному миру, безопасности и стабильности».[31]

Не все создаваемые угрозы одинаково опасны

Признать фундаментальное отсутствие безопасности в киберпространстве является необходимым первым шагом на пути к решению проблемы, но этого не достаточно для достижения решения. Эта уязвимость открывает дверь нескольким угрозам, каждая из которых ориентирована на различные части киберпространства, имеет разные цели, подвергает разным рискам национальную безопасность, и требует различных решений для их смягчения. Как и с другими проблемами кибербезопасности, никакого ясного консенсуса по вопросу о классификации этих угроз нет. Министерство обороны США, чьи усилия сконцентрированы на защите государственных компьютерных систем США, видит две основные категории угроз: сетевые компьютерные атаки (СКА) и использование компьютерных сетей в неблаговидных целях (ИКС).[32] Политолог Джозеф Най, придерживаясь более

---

[29] North Atlantic Treaty Organization, *Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization* (Brussels: NATO, 20 November 2010), 11; доступно на http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf.

[30] «Письмо, датированное 12 сентября 2011 года, от постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана к Организации Объединенных Наций, адресованное Генеральному секретарю»; шестьдесят шестая сессия Генеральной ассамблеи ООН, 14 сентября 2011.

[31] Министерство иностранных дел Российской Федерации, «Концепция внешней политики Российской Федерации», 12 февраля 2013; доступно на www.mid.ru/brp_4.nsf/0/76389FEC168189ED44257B2E0039B16D.

[32] Jayson M. Spade, *China's Cyber Power and America's National Security* (Carlisle, PA: U.S. Army War College, 2012), 7.

широкой и полезной точки зрения на опасности в киберпространстве, видит четыре вида деятельности, которые угрожают национальной безопасности: шпионаж, преступления, война и терроризм.[33]

Война и терроризм являются потенциально наиболее разрушительными угрозами в киберпространстве, и они близко коррелируют с категорией кибератака Министерства обороны США. Организация, которая занимается защитой от таких угроз наряду с защитой компьютерных сетей, связанных с обороной, это учрежденное недавно Киберкомандование Вооруженных сил США (USCYBERCOM). Однако правомочия USCYBERCOM простираются только до защиты некоторых частей федеральной государственной системы США; оно не несет никакой ответственности за большинство гражданских федеральных государственных систем, штатских или местных государственных сетей, или какой бы то ни было цифровой инфраструктуры в частном секторе, или в транспортных системах, энергетических системах, финансовых системах или системах коммуникации, которыми эти цифровые системы управляют.[34] Бремя ответственности за обеспечение безопасности невоенной части государственной федеральной системы несет Министерство внутренней безопасности, но нет ни одного федерального агентства, которое отвечало бы за обеспечение безопасности наиболее критической частной инфраструктуры от угроз кибератак.[35] Для альянса НАТО в целом ответственность раздроблена подобным образом, причем страны-члены отвечают за безопасность своих собственных сетей, а ответственность НАТО начинается с точек, где национальные сети и сети НАТО соединяются в общие для всего альянса сети.[36]

Шпионаж и киберпреступления могут и являются менее разрушительными угрозами, чем кибервойна или террористические нападения, но сейчас это наибо-

---

[33] Nye, *Cyber Power*, 16.

[34] Richard A. Clarke, "War from Cyberspace," *The National Interest* (November/December 2009): 33–34.

[35] Там же, 34–35. Недавно исполнительным приказом были расширены программы для взаимного предоставления информации о киберугрозах между федеральным правительством и частным сектором, установлено добровольное применение лучших практик в сфере кибербезопасности для поставщиков критической инфраструктуры, и было потребовано создать стимулы для поощрения стремления соответствовать стандартам. Смотри Office of the President of the United States, "Executive Order – Improving Critical Infrastructure Cybersecurity," 12 February 2013; доступно на www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity. Однако, при нежелании или неспособности Конгресса США принять такие законы как Закон о предоставлении разведывательной информации, связанной с кибербезопасностью и киберзащитой (CISPA), или Закон о кибербезопасности от 2012 года, чтобы узаконить программы предоставления информации и технические стандарты по кибербезопасности, многие из очевидных слабостей остаются без внимания.

[36] North Atlantic Treaty Organization, "Defending the Networks: The NATO Policy on Cyber Defence," 4 October 2011; доступно на http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf.

лее дорогостоящие угрозы безопасности, с которыми сталкиваются США.[37] Киберпреступления стали высокоорганизованной и феноменально выгодной незаконной деятельностью, при которой современные международные бизнес-практики сочетаются с самими передовыми технологиями, чтобы обогнать попытки корпораций и правоохранительных органов бороться с этой угрозой.[38] Фирма McAfee, занимающаяся безопасностью Интернета, в одном часто цитируемом докладе приводит оценку, что при киберпреступлениях в 2008 году была украдена в виде данных и интеллектуальной собственности пугающая сумма в 1 триллион долларов США.[39] Одна из конкурирующих фирм, Symantec, опубликовала в своем докладе за 2012 год более умеренную и консервативную оценку, что потери в результате киберпреступности составляют 110 миллиардов.[40] Отсутствие согласия о том, что является киберпреступлением, в сочетании с неустановленной формой протокола докладов о киберпреступлениях затрудняет оценку масштаба проблемы, но примерный порядок очевиден – он огромен.[41] В большинстве стран, в том числе и США, несмотря на ее масштаб, киберпреступность не воспринимается как прямая угроза для национальной безопасности, и следовательно, не является проблемой, которой занимается оборонный истэблишмент. Оставленное в целом в руках сообщества правоохранительных органов, международное сотрудничество нерегулярно, несмотря на то, что первая международная конвенция по киберпреступности была подписана десяток лет назад. К сожалению, многие из стран, где уровень киберпреступности самый высокий, и прежде всего Россия, не приняли международные нормы, касающиеся киберпреступности, и у них отсутствует же-

---

37 Nye, *Cyber Power*, 16.

38 Clay Wilson, "Cyber Crime," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz (Washington, D.C.: National Defense University Press, 2009), 415.

39 McAfee and SAIC, *Underground Economies: Intellectual Capital and Sensitive Corporate Data Now the Latest Cybercrime Currency* (28 March 2011), 5; доступно на www.ndia.org/ Divisions/Divisions/Cyber/Documents/rp-underground-economies.pdf. В кругах, связанных с кибербезопасностью, эта оценка воспринимается неоднозначно, потому что число шокирующе большое и потому, что эти числа последовательно повторялись в речах президента Обамы, генерала Александера из CYBERCOM и членами конгресса. Анализ оценки потерь в 1 триллион долларов можно найти среди прочих источников и в Misha Glenny, "Why You Can't Trust the Cybercrime Stats," *Wired UK* (6 November 2011); доступно на www.wired.co.uk/magazine/ archive/2011/12/ideas-bank/cybercrime-stats. Смотри так же Andy Greenberg, "McAfee Explains the Dubious Math behind Its 'Unscientific' $1 Trillion Data Loss Claim," *Forbes* (3 August 2012); доступно на www.forbes.com/ sites/andygreenberg/2012/08/03/mcafee-explains-the-dubious-math-behind-its-unscientific-1-trillion-data-loss-claim; и Peter Maass and Megha Rajagopalan, "Does Cybercrime Really Cost $1 Trillion?" *Pro Publica* (1 August 2012); доступно на www.propublica.org/article/ does-cybercrime-really-cost-1-trillion.

40 Symantec, *2012 Norton Cybercrime Report* (5 September 2012), 3; доступно на www.norton.com/2012cybercrimereport.

41 Wilson, "Cyber Crime," 428–29.

лание или способность ограничить криминальную онлайн деятельность на их территориях.

С другой стороны, кибершпионаж, близко связанный с киберпреступностью, является объектом, который находится в центре внимания министерств обороны повсюду в мире. Однако, разница между коммерческим кибершпионажем, который часто рассматривается как форма киберпреступности, и шпионажем, связанным с обороной, не всегда очевидна. Кибешпионаж в целом является значительной угрозой, но борьба с ним проблематична, поскольку на самом основном уровне шпионаж практикуется широко, и по международным законам не является незаконным.[42] Нации вели шпионскую деятельность с самых древних времен, и для них существует мало стимулов, чтобы ограничить деятельность, способствующую укреплению национальной безопасности и международной стабильности. Однако, у кибершпионажа есть характерные особенности, которые отличают его от традиционного шпионажа. Поскольку он «во много раз легче, дешевле, успешнее и у него мало отрицательных последствий [для страны, занимающейся им]»,[43] все больше стран принимает в нем участие, и делают они это все чаще.[44] Даже сейчас годовые потери от кибершпионажа огромны. Что однако более важно, чем финансовые потери, это то, что бесценная интеллектуальная собственность переходит к потенциальным противникам, и в частности к таким технологически развитым потенциальным равным конкурентам как Китай и Россия. Глава киберкомандования США, генерал Кейт Александер, в своей речи от 2012 года в Американском институте предпринимательства,[45] обозначил потери, как «самый большой трансфер богатства в истории», а бывший сотрудник Белого дома, Ричард Кларк, писал о своем опасении, что они могут «сдвинуть баланс могуществ в мире в сторону от Америки». [46]

Как отличия между кибершпионажем и киберпреступностью являются незначительными, так и отличия между кибершпионажем и атаками в киберреальности имеют очень тонкую грань.[47] Действительно, вторжение в компьютерную сеть для совершения атак, на начальных этапах выглядит практически идентичным акту шпионажа,[48] и код, оставляемый в системе злоумышленниками, который позво-

---

[42] James Lewis, "Five Myths about Chinese Hackers," *Washington Post* (22 March 2013).

[43] Clarke and Knake, *Cyber War*, 232.

[44] Там же, 228–37.

[45] Gen. Keith Alexander, "Cybersecurity and American Power," Keynote Address to the American Enterprise Institute, 9 July 2012; доступно на http://www.aei.org/events/2012/07/09/cybersecurity-and-american-power/.

[46] Clarke and Knake, *Cyber War*, 237; Greg Masters, "Global Cybercrime Treaty Rejected at U.N.," *SCMagazine* (23 April 2010); доступно на www.scmagazine.com/global-cybercrime-treaty-rejected-at-un/article/168630/.

[47] Andrew Cutts, "Warfare and the Continuum of Cyber Risks: A Policy Perspective," in *The Virtual Battlefield: Perspectives on Cyber Warfare*, ed. Christian Czosseck and Kenneth Geers (Amsterdam: IOS Press, 2009), 69.

[48] Libicki, *Cyberdeterrence and Cyberwarfare*, 16.

ляет дальнейший шпионаж, практически неотличим от программ, внедряемых для нанесения ущерба системе при последующей атаке.[49] Каждая попытка получить доступ к системе без соответствующей авторизации – по ошибке, из любопытства или в неблаговидных целях – почти неотличима для системных администраторов, которые отвечают за защиту системы, и большое число попыток затрудняет идентификацию серьезных угроз на фоне белого шума нормальной системной активности. В одной речи в 2010 году генерал Александер заявил, что «системы Министерства обороны являются объектом для попыток проникновения примерно 250 000 раз в час, более 6 миллионов раз в сутки».[50] Хотя не обязательно каждая такая попытка является компьютерной атакой, за исключением наиболее серьезных, сам объем потенциально опасной активности требует внимания и стал причиной поиска соответствующих решений.

И последнее усложнение, просто распознавание – и классификация – угрозы в киберпространстве уже является вызовом, но идентификация источника угрозы часто бывает еще более сложной проблемой. Найти ответственного за любую активность в киберпространстве неимоверно трудно. Каждый актор в киберпространстве может спрятаться за вуалью анонимности благодаря слабым требованиям стандартов авторизации и верификации самоличности пользователя, и эта анонимность усиливается технической легкостью, с которой можно замаскировать идентичность пользователя, его местоположение или маршрутизацию его онлайн активности.[51] В практическом смысле, это дает злонамеренным акторам в киберпространстве практически иммунитет от раскрытия, так как текущие технологии цифрового криминалистического расследования часто не в состоянии обеспечить бесспорные доказательства идентичности. Это так же делает определение ответственности государств за деятельность в киберпространстве трудоемким предприятием, так как правительства могут правдоподобно отрицать причастность к действиям, которые, похоже, исходят из действий на территории их страны, но это нельзя однозначно доказать.[52]

---

[49] Libicki, *Cyberdeterrence and Cyberwarfare,* 24–25; Clarke, "War from Cyberspace," 33–34.

[50] Gen. Keith Alexander, "U.S. Cybersecurity Policy and the Role of U.S. CYBERCOM," CSIS Cybersecurity Policy Debate Series (3 June 2010), 6; доступно на http://csis.org/files/attachments/100603csis-alexander.pdf.

[51] Geers, *Strategic Cyber Security*, 95.

[52] Определение ответственности государства за киберинцидент включает два компонента: степень участия и степень уверенности в участии. Каждое из этих измерений сравнивается со шкалой в диапазоне от низкой до высокой, что означает, что внешний наблюдатель может определить варьирующие степени участия государства в деятельность, стоящую за инцидентом, и может сделать это с разной степенью уверенности. Чем больше уверенность в участии данного государства и выше степень этого участия, тем большую ответственность несет это государство за данный инцидент.

Нет простых решений

Несмотря на серьезность уязвимости в киберпространстве, нахождение решений не есть простая задача. Эта проблема похожа на сеть гордиевых узлов, часто требует применения интердисциплинарных подходов, в которых сочетаются сложные решения с техническими, юридическими и политическими компонентами и часто имеются непреднамеренные последствия в *terra incognita* киберпространства.[53] Сложность, переплетение проблемных областей, трудность координации и стандартизации ответственности за разрешение проблем приводит к медленному прогрессу как на национальном, так и на интернациональном уровне.

Возможно, наибольшим вызовом является отсутствие международного правового режима или каких бы то ни было общепринятых норм для киберпространства, либо в варианте расширенных приложений существующих правил, либо полученные в результате создания новых рамочных документов для этой специфической сферы.[54] Этот пробел является функцией отсутствия четкого свода законов, который незамедлительно транслируется к новым вызовам, появляющимся в киберпространстве, заодно с растущей важностью киберпространства, которая намного обгоняет ледниковую скорость создания международных правовых стандартов.[55] Без таких рамочных документов дискуссии между национальными государствами о том, что является приемлемым поведением, остаются в большей степени теоретическими, чем практическими, и перечень неразрешенных проблем заставляет нас широко раскрывать глаза в удивлении. К примеру, вопрос об ответственности государства за злонамеренные действия, которые исходят или проходят через территорию страны, остается вопросом нерешенным и спорным.[56] Киберпреступность продолжает действовать без существенного противодействия, и ответственность за реакцию на трансграничные преступные действия не возлагается автоматически на государство или не принимается соответственно государством. Отсутствие универсального определения того, что является неприемлемым поведением, которое было бы законным *casus belli* (поводом для войны) между государствами, оставляет неопределенной черту, которую надо перейти, чтобы это привело к международному конфликту. И без режима, который гарантировал бы наказательные последствия за плохое поведение, будет почти невозможно предот-

---

[53] Maeve Dion, "Different Legal Constructs for State Responsibility," in *International Cyber Security Legal & Policy Proceedings 2010*, ed. Eneken Tikk and Anna-Maria Talihärm (Tallinn, Estonia: Cooperative Cyber Defence Center of Excellence, 2010), 69.

[54] *Таллиннское руководство* – это рецензируемое коллегами, но не официальное издание, которое пытается устранить этот серьезный недостаток с помощью международной группы экспертов, интерпретирующих существующее международное право в киберконтексте. Изданию меньше года, и итоговое влияние этого документа все еще предстоит определить. Смотри Michael N. Schmitt, gen. ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013).

[55] Rex Hughes, "A Treaty for Cyberspace," *International Affairs* 86:2 (2010): 533.

[56] Goodman, "Cyber Deterrence," 112–13.

вращать приводящие к ущербу или провокационные действия, которые являлись бы отклонением от стандартов поведения или даже прямой угрозой миру.[57]

Кроме того, национальные рамочные документы, регламентирующие действия, связанные с киберпроблемами, начиная от документов по борьбе с преступностью, относящиеся к шпионажу, и кончая военной доктриной, часто неполны, устарели или неадекватны. Некоторые национальные своды законов не могут обеспечить даже основные инструменты для борьбы с цифровым мошенничеством и цифровыми кражами, не говоря уже о более изощренных или новопоявляющихся криминальных угроз. Даже наиболее передовые национальные стратегии и рамочные документы содержат пробелы или допускают компромиссы в поиске разных способов обеспечить баланс, к примеру, в распределении ответственности за кибербезопасность между государством и частным сектором, или между относительной значимости безопасности и гражданскими свободами.[58] Эта национальная политика, в свою очередь, плохо гармонизирована в международном плане, даже между близкими партнерами из-за отсутствия глобальных норм и различающихся национальных приоритетов.

Различия в приоритизации повестки дня международной кибербезопасности проистекают из фундаментально различающегося понимания природы киберпространства и приемлемого поведения в кибердомейне. Некоторые государства, такие как Китай и Россия, считают, что существующее международное законодательство неадекватно, и выступают за новый международный договор, который будет третировать специально операции в киберпространстве, ставят суверенность выше международного сотрудничества и рассматривают содержание Интернета как потенциальную угрозу для их политической стабильности, которое требует жесткого контроля. Другая сторона в споре, наиболее развитые демократии, придерживаются мнения, что международное право может быть эффективно применено к киберпроблемам, считают, что новый договор о киберправе не нужен, приветствуют международное сотрудничество даже если при этом приходится поступаться своим суверенитетом и рассматривают доступ к Интернету и свободный поток информации в качестве фундаментальных прав. Эти несовместимые точки зрения усложняют создание международных законов по киберпроблемам и препятствуют почти всем дискуссиям по этой материи, так как ключевые игроки с трудом находят общую почву для сотрудничества даже по самым фундаментальным проблемам.[59]

---

[57] Lewis, “Rethinking Cyber Security.”

[58] Репозиторий национальных стратегий и политик можно найти на вебстранице Совместного центра НАТО повышения квалификации в сфере кибероборонbы http://ccdcoe.org/328.html.

[59] Carr, *Inside Cyber Warfare* (Sebastopol, CA: O’Reilly Media, 2010), 34–35. Относительно представительных примеров смотри Masters, “Global Cybercrime Treaty Rejected at U.N.” Институт Восток-Запад и Институт информационной безопасности Московского Государственного Университета сотрудничали в усилиях по Дорожке 2, направленных на разработку консенсусной терминологии для кибербезопасности. Первый круг их работы

В результате отсутствия международных норм и несоответствия национальных рамочных документов в области киберпроблем «плохие акторы» в киберпространстве, кто бы они не были – государства, группы или отдельные индивиды – часто действуют вне досегаемости пострадавших, которые пытаются реагировать в ответ или получить возмещение нанесенного им ущерба. Недостатки такого характера создают пробелы, которыми пользуются, и приводят к трениям между сторонами. В некоторых случаях безопасность бывает настолько нарушена, что вспыхивает конфликт.

Когда меры безопасности не работают

Несмотря на относительную новизну киберпространства, большое количество стоящих упоминания инцидентов в широком диапазоне сферы кибербезопасности привлекает общественное внимание. Полный спектр потенциальных угроз национальной безопасности в киберпространстве может быть еще и не вполне очевиден, но краткий обзор основных инцидентов показывает, как увеличивающуюся серьезность, так и большое разнообразие угроз с последствиями для национальной безопасности, многие из которых уникальны в историческом плане и являются новыми прецедентами или являются новыми вызовами для международного сообщества.

Ранние и с относительно нетяжелыми последствиями инциденты в сфере кибербезопасности имели место еще во времена Холодной войны, когда Соединенные Штаты, по имеющимся сведениям, провалили советскую шпионскую операцию, позволив кражу компонентов системы управления нефтепроводов с использованием злонамеренного программного обеспечения, что в итоге привело к последующему зрелищному отказу нефтепровода, вызвавшего огромный взрыв, самый большой неядерный взрыв, который когда-либо имел место.[60] Во время Второй Интифады на Палестинской территории в 2000 году хакеры израильского правительства отключили публичные веб-страницы Палестинской национальной администрации и Хезболла в попытке нарушить командование и управление восстания. Палестинские оперативники ответили кибератаками против израильских банков и правительственных компьютерных систем, что вызвало нечто как «свя-

привел к согласию по двадцати базовым терминам в апреле 2011; смотри Karl Frederick Rauscher and Valery Yashchenko, "Russia-US Bilateral on Cyber Security: Critical Terminology Foundations," April 2011; доступно на www.ewi.info/system/files/reports/Russia-U%20S%20%20bilateral%20on%20terminology%20v76%20%282%29.pdf. Выполняется последующая программа на дальнейшее согласованное расширение лексикона.

[60] Clarke and Knake, *Cyber War*, 92–93. Другие источники оспаривают этот доклад, к примеру, Jeffrey Carr, "The Myth of the CIA and the Trans-Siberian Pipeline Explosion," *Digital Dao* (7 June 2012); доступно на http://jeffreycarr.blogspot.com/2012/06/myth-of-cia-and-trans-siberian-pipeline.html.

щенную кибервойну».[61] Израиль так же использовал наступательные кибертехнологии, чтобы обмануть сирийские радары противовоздушной обороны, как часть операции по бомбардировке израильскими военно-воздушными силами предположительного сирийского ядерного сооружения в сентябре 2007 года.[62]

Продолжительная тайная шпионская операция, известная как «Титановый дождь», имела место с 2003 по 2005 год, в рамках которой происходило систематическое инфильтрирование в государственные компьютерные системы США и Западной Европы.[63] Многие считают, что это была программа китайского правительства, в результате которой были получены от десяти до двадцати терабайт данных только из сетей вооруженных сил США.[64] Попытки блокировать проникновения в процессе их осуществления часто были неуспешными, и прикрытый характер вторжений делал даже идентификацию времени, продолжительности атаки и украденных данных делом догадок экспертов.[65] Похоже, что «Титановый дождь» являлся частью более широкой, долгосрочной работы Китая по кибершпионажу, иногда обозначаемой как Передовая Постоянная Угроза (ППУ), и последующих подобных операций, ответственность за которые возлагается на Китай, включающих взлом компьютерных систем членов конгресса США и обширную эксфильтрацию очень чувствительных проектов для передовой программы Совместного Ударного Истребителя F-35 военного контрактора США Локхид Мартин.[66] Хотя «Титановый дождь» и связанные шпионские программы почти наверняка исходят из Китая, упорное отрицание Китая не является ни неожиданным, ни необычным, имея в виду, насколько трудно однозначно возложить на кого-то ответственность в киберпространстве. Подобным образом уязвимость, в смысле кражи или повреждения даже наиболее чувствительных данных и высокая эффективность программ кибершпионажа при сравнительно низком уровне риска приводят к тому, что такие операции без цивилизующего влияния неявных правил дорожного движения, развывшихся для регламентирования традиционного шпионажа, будут повторяться все чаще.[67]

Первый большой межгосударственный киберконфликт начался в апреле 2007 года, когда эстонское правительство перенесло советский мемориал Второй мировой войны с его центрального местоположения в середине столицы Таллинна на военное кладбище за пределами городского центра. Это решение стало причиной громкой реакции со стороны России и этнического русского меньшинства в Эсто-

---

[61] Kenneth Geers, "Cyberspace and the Changing Nature of Warfare," *SC Magazine* (27 August 2008); доступно на www.scmagazine.com/cyberspace-and-the-changing-nature-of-warfare/article/115929/.

[62] Clarke and Knake, *Cyber War*, 1–11.

[63] Brian M. Mazanec, "The Art of (Cyber) War," *Journal of International Security Affairs* (Spring 2009); доступно на www.securityaffairs.org/issues/2009/16/mazanec.php.

[64] Carr, *Inside Cyber Warfare*, 4.

[65] Clarke and Knake, *Cyber War*, 124–26.

[66] Spade, *China's Cyber Power*, 5.

[67] Nye, "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* (Winter 2011): 31.

нии, эскалировавшее в насильственные столкновения между приверженцами обеих сторон спора и быстро перешедшее в массовые беспорядки и грабежи в центре Таллинна. Столкновения перенеслись в киберпространство, в котором сильно цифровизированная Эстония была исключительно уязвима в отношении своих государственных вебсайтов, вебсайтов органов правопорядка и веб-сайтов средств массовой информации, и продолжались в течение трех недель в виде все более интенсивных и хорошо скоординированных компьютерных атак.[68] Хотя кибернападения скорее создали некоторые неудобства, чем стали причиной реального ущерба, этот инцидент явился показательным в нескольких аспектах.[69] Это была первая массовая атака, направленная на управление государства и на промышленность, и как часть международного конфликта она оказалась достаточно серьезной для того, чтобы дать Эстонии основание потребовать консультации с союзниками по НАТО согласно положениям Атлантического Договора.[70] Он поднял важные вопросы о порогах степени применения силы и вооруженных нападений согласно международному праву.[71] Хотя Россия отрицала, что несет ответственность за это, и цифровое криминалистическое расследование не смогло однозначно доказать, что за атакой стояло российское государство, совокупность свидетельств дает основание предположить, что российское государство по крайней мере поощряло, а возможно и осуществляло руководство атаками.[72] У российского правительства в данном случае есть повод отрицать свою причастность к инциденту благодаря участию «патриотических хакеров», которые, по мнению российского руководства, являются просто разгневанными, интернет-грамотными гражданскими активистами, мобилизовавшими и организовавшими себя самостоятельно для выполнения хорошо скоординированных атак против специфических Интернет целей, используя десятки тысяч взломанных компьютеров из 177 стран

---

[68] Geers, *Strategic Cyber Security*, 84–86.

[69] Rain Ottis, "Case Studies on Cyber Conflict – Estonia 2007 and Stuxnet 2010," Presentation at the George C. Marshall European Center for Security Studies, Garmisch-Partenkirchen, Germany, 22 October 2012.

[70] Улф Хойслер уточняет, что единственные официальные консультации с членом Северо-Атлантического Совета (САС) согласно положениям Северо-Атлантического Договора были проведены, когда Турция потребовала этого в феврале 2003 года, перед возобновлением враждебных действий против Ирака. Хотя дискуссии в САС в 2007 году проходили в контексте кибератак в Эстонии, ни Совет, ни Эстония явным образом не упомянули статью 4 в связи с разговорами. Смотри Häußler, "Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO Treaty," in *International Cyber Security Legal & Policy Proceedings 2010*, ed. Christian Czosseck and Karlis Podins (Tallinn, Estonia: Cooperative Cyber Defence Center of Excellence, 2010), 104–5.

[71] Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," *Berkeley Journal of International Law* 27 (2009): 196–97.

[72] Kara Flook, "Russia and the Cyber Threat," American Enterprise Institute Critical Threats (13 May 2009); доступно на www.criticalthreats.org/russia/russia-and-cyber-threat. Смотри так же Carr, *Inside Cyber Warfare*, 3; и Goodman, "Cyber Deterrence," 111.

без какой-либо государственной поддержки или помощи.[73] Отрицание ответственности, ставшее обычным в последующих случаях, подчеркивает сложность проблемы возложения ответственности на государство в киберпространстве. Так же проливается свет на вызовы, которые снова будут появляться в следующих киберинцидентов.

Во время войны в августе 2008 года между Россией и Грузией кибератаки, синхронизованные с наземными и воздушными операциями российской армии, парализовали грузинский интернет домен «.ge», переполнив системные серверы неуправляемым потоком веб-трафика. Государственные, банковские и сайты средств массовой информации были заблокированы, и даже национальная сеть мобильной телефонной связи была выведена из строя.[74] Наиболее значительным последствием этой атаки было лишение грузинского правительства способности коммуникировать эффективно, – в особенности, оно было лишено возможности показать события во время военных действий со своей точки зрения, – а так же нарушения публичных услуг, в частности банковской деятельности, электроснабжения и телекоммуникаций.[75] Как и при эстонском инциденте, Россия категорически отрицала ответственность государства за киберкомпонент войны, хотя, без всякого сомнения, воспользовалась стратегическими преимуществами, проистекшими из кибератак на Грузию,[76] а организаторы атак определенно знали заранее о наземной войне и получили содействие (если не руководство) при планировании, организации, рекогносцировке и синхронизации их действий с действиями российских вооруженных сил.[77]

Одна наиболее узко направленная кибероперация, раскрытая в 2010 году, пролила свет на более новую и менее публичную форму киберконфликта. Тайная совместная операция США и Израиля, под названием «Олимпийские игры», была направлена на подрыв иранской ядерной программы.[78] Один из компьютерных вирусов, использованных в операции «Олимпийские игры», под названием Stuxnet, содержал программный код, который находил определенное программное обеспечение и аппаратные конфигурации, характерные для иранских сооружений для обогащения урана. Найдя правильную комбинацию, он брал на себя управление оборудованием и заставлял его работать вне нормального диапазона стоимостей параметров, срывая процесс обогащения, повреждая оборудование и вызывая замешательство среди ученых и администраторов, ведущих программу.[79] По мне-

[73] Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents: Legal Considerations* (Tallinn, Estonia: Cooperative Cyber Defence Center of Excellence, 2010), 18–25.
[74] Clarke and Knake, *Cyber War*, 17–21.
[75] Tikk, Kaska and Vihul, *International Cyber Incidents*, 77–79; Goodman, "Cyber Deterrence," 115.
[76] Carr, *Inside Cyber Warfare*, 15–19.
[77] Flook, "Russia and the Cyber Threat."
[78] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times* (1 June 2012).
[79] Ottis, "Case Studies on Cyber Conflict"; Sanger, "Obama Order."

нию бывшего директора ЦРУ и генерала в отставке военно-воздушных сил В. Хейдена, Stuxnet был «первым случаем значительного масштаба, при котором кибератаки использовались для причинения физических разрушений». «Кто-то перешел Рубикон».[80] Действительно, Stuxnet был технологически инновационным и обозначил водораздел в смысле причинения физического ущерба, который, возможно, превышал законодательный порог, означающий применение вооруженной силы, и даже порог вооруженного нападения, согласно международному праву. Однако, поскольку США и Израиль никогда официально не признали свою роль в этой операции, данный инцидент снова поднимает вопрос об атрибуции и ответственности государства и усиливает необходимость в согласованных коллективных действиях для разрешения проблем кибербезопасности.

Роль России

Россия, несмотря на все ее проблемы, все еще играет значительную роль в международной системе. По разным причинам, она располагает достаточной силой в своем постсоветском перевоплощении, чтобы иметь решающее влияние на жизненно важные для международного сообщества проблемы. Хотя ее отношения с США, Европой и ее соседями на постсоветском пространстве иногда бывают сложными, сочетание физических размеров Российской федерации, ее геостратегического положения, военных мускулов, экономического могущества, природных ресурсов и других факторов требуют, чтобы с Россией считались или даже советовались при разрешении почти каждой проблемы на международной повестке дня.[81] Во многих случаях Россия оказывает достаточное влияние, чтобы определять, когда и как будут решаться проблемы – или они будут продолжать гноится. Несмотря на эту критически важную роль, или возможно, как раз из-за нее, Соединенные Штаты и их союзники по НАТО пытаются поддерживать стабильно хорошие, продуктивные и способствующие сотрудничеству связи с Москвой, и констатируют, что практически невозможно превратить эти отношения в устойчивое и значимое партнерство, которое приносило бы выгоду из-за их глубокой взаимозависимости и множеству вопросов, по которым их интересы пересекаются.

В своем радиообращении по Би-Би-Си в 1939 году Уинстон Черчилль дал следующий широко известный комментарий: «Я не могу предсказать действия России. Это загадка, завернутая в тайну среди енигмы, но возможно и существует ключ. Этот ключ – национальные интересы России».[82] Проницательное наблюдение Черчилля также не менее верно и сегодня, чем оно было три четверти века

[80] Sanger, “Obama Order.”

[81] Stephen J. Blank, “Introduction,” in *Prospects for U.S.-Russian Security Cooperation*, ed. Stephen J. Blank (Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 2009), 1.

[82] Winston Churchill, “The War Memoirs of Winston Churchill,” *Life Magazine* (10 May 1948): 63.

назад. Россия, как и большинство стран, будет действовать в собственных интересах – или в лучших интересах своего национального руководства. Тем не менее, понять, каковы интересы России и предсказать, как Россия будет себя вести, чтобы их обеспечить, совсем нелегкая задача.[83] Непознаваемая русская психология оказывает влияние на принятие внешнеполитических решений, так как российские руководители пытаются восстановить национальный престиж и заново заслужить уважение международного сообщества, демонстрируя силу, напористость и решительность в своих внешних отношениях. Вне России этот подход часто воспринимается как высокомерие и даже агрессивность российского поведения, что ведет к бурным отношениям и предельно неустойчивым моделям взаимодействия с другими странами.[84]

Несмотря на отсутствие видимых экзистенциальных угроз для Российской Федерации, российские политики часто демонстрируют отношение незащищенности от внешних угроз и рассматривают международное окружение как инкубатор для потенциальных опасностей.[85] Это мировоззрение – и его несовпадение с представлением большой части остального мира о ситуации с безопасностью России – объясняет многие из шероховатостей, проистекающих из внешней политики России. Рассматриваемые с этой точки зрения, последовательные усилия России обеспечить себе влияние на «ближнее зарубежье», состоящее из бывших советских республик, и защищаться от того, что она воспринимает как недопустимое вмешательство таких внешних сил, как США, Китай и Европа, направлены на стабилизацию своей периферии, создание буферов против внешних угроз и обеспечение возможности стране сосредоточиться на своих внутренних проблемах.[86] Также Россия категорически не согласна с расширением НАТО в Восточной Европе и на пространстве бывшего Советского Союза, причем особенно жесткие возражения вызвали дискуссии о членстве Украины и Грузии на Бухарестском саммите НАТО в 2008 году. Хотя беспристрастный анализ показал бы, что НАТО является моделью институции безопасности, которая обеспечивает региональную стабильность, что должно быть выгодно Российской Федерации, мнение России о НАТО совсем другое, она рассматривает его в качестве потенциальной угрозы и исторического соперника, который подкрадывается к жизненно важным террито-

[83] Samuel A. Greene and Dmitri Trenin, (*Re) Engaging Russia in an Era of Uncertainty*, Policy Brief 86 (Washington, D.C.: Carnegie Endowment for International Peace, December 2009), 4; Andrei Shleifer and Daniel Treisman, "Why Moscow Says No," *Foreign Affairs* (January/ February 2011): 122–38.

[84] David J. Kramer, *The Russia Challenge: Prospects for US-Russian Relations*, Policy Brief (Washington, D.C.: The German Marshall Fund, 2009), 2.

[85] Olga Oliker, Keith Crane, Lowell H. Schwartz, and Catherine Yusupov, *Russian Foreign Policy: Sources and Implications* (Santa Monica, CA: RAND Project Air Force, 2009), 2 and 83–84.

[86] R. Craig Nation, *Results of the "Reset" in US-Russian Relations*, Russie.Nei.Visions No. 53 (Paris: IFRI, 2010), 9; Oliker, et al., *Russian Foreign Policy*, 93–95.

риям на российской границе и угрожает России окружением.[87] Инициатива Европейского Союза Восточное партнерство так же была встречена Россией скептически, поскольку Москва придерживается мнения, что эта инициатива является попыткой заманить несколько бывших советских республик уйти с орбиты российского влияния.[88]

Эти давние сложности в течение многих лет сопровождались трениями по поводу разных проблем, в число которых в последнее время входили планы США создания новой ПРО, усилия по развитию демократии,[89] публичное осуждение неудовлетворительного состояния прав человека в России[90] и разногласия по Ливии, Сирии и Ирану.[91] Отношения с Западом достигли свей самой низкой точки во время войны России с Грузией в августе 2008 года, когда репутация России понесла серьезный урон, и сотрудничество между Западом и Россией практически было приостановлено.[92] После нескольких месяцев тупиковой ситуации, в феврале 2009 года вице-президент США Джозеф Байден озвучил желание администрации Обамы «нажать на кнопку перезагрузки» отношений с Россией и остановить «опасный дрейф», и обратил внимание на перечень общих интересов, в том числе нераспространение ядерного оружия, борьбу с международным терроризмом и стабильность в Афганистане.[93]

Результаты перезагрузки были неоднозначными. Некоторые эксперты считают, что добрые намерения были осуществлены, поскольку наметилось потепление отношений между США и Россией, возобновилось сотрудничество в отношении Афганистана, санкций против Ирана, принятия России в ВТО и по новому договору о сокращении стратегических вооружений.[94] Другие наблюдатели менее воодушевлены и указывают на постепенное размывание первоначальных надежд на перезагрузку в результате разногласий по Ирану и Сирии, неясности о легитимности победы Путина на президентских выборах в 2012 году, принятие Закона Маг-

---

87 Linas Linkevicius, "Reset with Russia, but with Reassurance," *International Herald Tribune* (9 September 2010); Nation, *Results of the "Reset*," 13-14; Shleifer and Treisman, "Why Moscow Says No."

88 Kramer, *The Russia Challenge*, 4.

89 Oliker, et al., *Russian Foreign Policy*, xvi.

90 Commission on U.S. Policy toward Russia, *The Right Direction for U.S. Policy toward Russia* (Washington, D.C.: The Nixon Center, March 2009), 13–14; Dmitri Trenin, et al., *The Russian Awakening* (Moscow: Carnegie Moscow Center, 2012), 8.

91 Nation, *Results of the "Reset,"* 23; David M. Herszenhorn and Nick Cumming-Bruce, "Putin Defends Stand on Syria and Chastises U.S. on Libya Outcome," *The New York Times* (21 December 2012).

92 Robert Coalson, "Former U.S. State Dep't Official Pifer Asks, 'Are the Russians Ready to Reengage?'" *Radio Free Europe/Radio Liberty* (19 November 2012).

93 Craig Whitlock, "'Reset' Sought on Relations with Russia, Biden Says," *Washington Post* (8 February 2009).

94 Стивен Сестанович, интервью с Бернардом Гвертцманом «Заново оценивая «Перезагрузку» США-Россия», веб-сайт Совета по иностранным отношениям (13 декабря 2012); доступно на www.cfr.org/ russian-federation/reassessing-us-russia-reset/p29659.

нитского в США о санкциях для российских чиновников, которые нарушают права человека, российских военных учений, симулирующих вторжение в Польшу и т.д.[95] Возможно, конечный итог перезагрузки никогда не станет ясным, но необходимость для США и НАТО продолжать политику взаимодействия с Россией остается неизменной.

При наличии отношений, которые все более взаимозависимы и интересов, которые сходятся по многим вопросам, США и НАТО ясно понимают, что сотрудничество с Россией необходимо, а отсутствие сотрудничества обойдется дороже.[96] После двусторонней встречи в 2012 году с Дмитрием Медведевым, в то время президентом Российской Федерации, президент США Барак Обама подтвердил эту точку зрения, заявив, что «как для двух ведущих мировых сил, для нас является абсолютно критически важным эффективно коммуникировать и эффективно координировать свои действия в ответ на ситуации широкого спектра, угрожающие глобальному миру и безопасности …. В период больших изменений в мире сотрудничество между Соединенными Штатами и Россией критически важны для глобального мира и стабильности».[97] Также Стратегическая концепция НАТО от 2010 года подтвердила, что «Сотрудничество НАТО-Россия имеет стратегическое значение, так как оно способствует созданию общего пространства мира, стабильности и безопасности ... Мы убеждены, что безопасность НАТО и России неразрывно связаны, и что прочное и конструктивное партнерство, основанное на взаимном доверии, прозрачности и предсказуемости лучше всего способствует обеспечению нашей безопасности».[98] Россия, со своей стороны, придерживается более осторожного подхода, призывая в своей стратегии национальной безопасности к «равноправному и эффективному стратегическому партнерству с Соединенными Штатами Америки на основе общих интересов и с учетом ключевого влияния российско-американских отношений на международную ситуацию в целом» и обозначая свое желание «развивать отношения с НАТО на основе равенства и в интересах укрепления общей безопасности в Евро-Атлантическом регионе».[99]

---

[95] Anne Gearan, "Sour U.S.-Russia Relations Threaten Obama's Foreign Policy Agenda," *Washington Post* (14 January 2013); Thomas E. Graham and Dmitri Trenin, "Why the Reset Should Be Reset," *New York Times* (12 December 2012); и Shleifer and Treisman, "Why Moscow Says No."

[96] Blank, "Introduction," 16.

[97] Barack Obama and Dmitry Medvedev, "Remarks by President Obama and President Medvedev of Russia After Bilateral Meeting," 26 March 2012; доступно на www.whitehouse.gov/the-press-office/2012/03/26/remarks-president-obama-and-president-medvedev-russia-after-bilateral-me.

[98] North Atlantic Treaty Organization, *Active Engagement, Modern Defence* (Strategic Concept), 29–30.

[99] National Security Council of the Russian Federation. "Russia's National Security Strategy to 2020," 12 May 2009; доступно на http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020 (перевод на английский язык).

К сожалению, текущий стратегический диалог ограничен как в смысле обсуждаемых вопросов, так и в смысле конкретного прогресса по какому-либо вопросу на повестке дня. И США, и Россия, и НАТО страдают близорукостью в своем подходе к взаимодействию, занимаясь только узким кругом вопросов, не желая рисковать для достижения успеха и таким образом пропуская возможности достичь хотя бы минимальных успехов.[100] Этот неуспех разочаровывает, поскольку сотрудничество само по себе плодотворно, если оно ломает инерцию несговорчивости и порождает дальнейшее сотрудничество по уже обсуждаемым или другим наболевшим проблемам.[101] Ощутимого успеха достичь трудно, и найти дорогу к нему является основной целью, начиная, возможно, с маленьких побед, с укрепления доверия, с превращения сотрудничества в привычку, и только в итоге вплотную начав заниматься наиболее срочными задачами, но уже в качестве партнеров, которые доверяют друг другу. Поэтому четыре бывших посла США в Москве и четыре бывших советских и российских посла в Вашингтоне в письме, опубликованном ранее в этом году, высказали своим правительствам мнение, что надо приложить больше усилий в этом направлении, так как «более активный поиск возможностей для совместных проектов в областях общих взаимных интересов добавил бы важный элемент в структуре российско-американской стабильности».[102] Кибербезопасность является ключевой областью, в которой интересы США, НАТО и России совпадают и возможен быстрый прогресс, который станет основанием для дальнейшего взаимодействия и улучшения отношений в более широком плане между всеми участвующими в процессе сторонами.

Россия и кибербезопасность

Россия является весьма могущественной силой в киберсфере, которую Киберкомандование США оценивает, как «почти равную» США,[103] с более совершенными способностями, чем другие развитые конкуренты, например Китай и Израиль.[104] Эта способность является результатом того, что Россия богата высоко образованными кадрами с добротным техническим образованием, которые составляют

[100] Blank, "Introduction," 17; Oliker, et al., *Russian Foreign Policy*, 137; Sestanovich, "Reassessing the U.S.-Russia 'Reset'."

[101] Blank, "Introduction," 6.

[102] John Beyrle, et al. "Priorities for Russia-U.S. Relations: A Statement by Former Ambassadors to Washington and Moscow," Carnegie Endowment for International Peace Web Site (12 April 2013); доступно на http://carnegieendowment.org/2013/04/12/priorities-for-russia-u.s.-relations-statement-by-former-ambassadors-to-washington-and-moscow/fza1.

[103] Keir Giles, "'Information Troops' – A Russian Cyber Command?" in *3rd International Conference on Cyber Conflict*, ed. Christian Czosseck, Enn Tyugu, and Thomas Wingfield (Tallinn: CCD COE Publications, 2011), 50.

[104] James Fallows, "Cyber Warriors," *The Atlantic* (March 2010); доступно на www.theatlantic.com/magazine/archive/2010/03/cyber-warriors/307917/. Смотри так же David A. Fulghum, "China Cyber-skills Are Improving But Still Don't Top Russia and Israel," *Aviation Week* (28 March 2012).

большой резерв квалифицированного человеческого капитала, очень пригодного для найма на работу в предприятиях, связанных с информационными технологиями.[105] При отсутствии перспектив для этих талантов в не очень хорошо развитой технической индустрии России российские государственные компьютерные сети и компьютерные сети организованной преступности – которые, похоже, иногда тесно переплетаются в киберсфере[106] – стали самими большими рынками, предоставляющими прибыльную работу.[107]

Хотя Россия и располагает этой передовой способностью, находясь в числе лучших в мире, ее фундаментальное понимание кибербезопасноси весьма расходится с представлением в США и НАТО,[108] что создает философские и концептуальные различия, являющиеся реальными, хотя и преодолимыми препятствиями для конструктивного диалога по киберпроблемам. В настоящее время отсутствие общего понимания делает любую дискуссию между Россией и Западом по темам киберсферы, по словам одного эксперта, актом «взаимного непонимания и очевидной непримиримости».[109] Чтобы сотрудничество было плодотворным, эти различия надо понимать и преодолевать, что достижимо только путем регулярного диалога и постоянного взаимодействия. Эта точка зрения была отражена в высказывании координатора по кибервопросам государственного секретаря США Кристофера Пайнтера: «Нам необходимо привлечь к участию все страны мира, даже те, с которыми мы не согласны».[110]

Россия не рассматривает кибербезопасность или какую бы то ни было деятельность в киберпространстве как отдельную, изолированную проблему, в отличие от преобладающей тенденции на Западе. На самом деле, *кибер* – массовый термин на Западе – не используется в официальных документах на русском языке, за исключением случаев, когда речь идет о действиях других стран. Наоборот, тогда как западные эксперты обсуждают *кибер*, российское военное сообщество предпочитает использовать термин *информатизация*, рассматривая кибер проблематику как составную часть более широкой концепции информационных операций.[111] На

[105] Flook, "Russia and the Cyber Threat"; Fulghum, "China Cyber-skills Are Improving."

[106] Carr, *Inside Cyber Warfare*, 124–25; Flook, "Russia and the Cyber Threat"; Joshua McGee, "US-Russia Diplomacy – The "Reset" of Relations in Cyberspace," Center for Strategic and International Studies Web Site (5 August 2011); доступно на http://csis.org/blog/us-russia-diplomacy-reset-relations-cyberspace.

[107] Flook, "Russia and the Cyber Threat"; "Interview with Joseph Menn, Author of Fatal System Error," *Cyveillance* (2 June 2010); доступно на https://blog.cyveillance.com/general-cyberintel/fatal-system-error-joseph-menn.

[108] Jason Healey, "Comparing Norms for National Conduct in Cyberspace," *New Atlanticist* (20 June 2011); доступно на www.acus.org/new_atlanticist/comparing-norms-national-conduct-cyberspace

[109] Giles, "Russia's Public Stance on Cyberspace Issues," 64.

[110] Benjamin Boudreaux, "Cyber Diplomats," *State Magazine* (April 2013): 32.

[111] Timothy Thomas, "Nation-State Cyber Strategies: Examples from China and Russia," в *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, D.C.: National Defense University Press, 2009), 476.

самом деле, базовый документ для российской информационной безопасности не содержит ни слова *кибер*, ни слова *Интернет* в своем тексте.[112] Наоборот, русские придерживаются целостного, интегрированного подхода к информационным операциям (или информационной войне), который сочетает технические измерения, включающие аппаратные средства, программное обеспечение и другие технологические компоненты в психологическом аспекте, который оказывает влияние на обработку информации, восприятие, отношение и решения, которые обеспечивают России информационное преимущество перед ее конкурентами или противниками.[113] С русской точки зрения, технические измерения кибер проблематики – защиту данных и компьютерных систем от хакеров, шпионов и преступников – нельзя отделить от когнитивных аспектов использования информации, таких как связи с общественностью, психологические операции, дезинформация и т.д.[114]

Этот подход приводит к тому, что Россия концентрирует свои усилия в сфере национальной информационной безопасности на защите общества от «вредной» информации. Идея, что информацию можно считать опасной, высвечивает другое важное отличие между точками зрения России и Запада. Запад рассматривает информацию как общественное благо, которое государствам следует подвергать минимальному контролю и позволять ей течь настолько свободно, насколько это возможно, в том числе и в Интернете – то, что бывший государственный секретарь США Хиллари Клинтон назвала «свободой быть на связи».[115] Российская Федерация, наоборот, сильно беспокоится по поводу дестабилизирующего влияния неограниченного обмена информации на ее общество, или по крайней мере на правление нынешних властей.[116] «Интернет суверенитет», или способность государства перлюстрировать, и в случае необходимости контролировать, информационный домен является до сих пор существенным элементом российской позиции по кибербезопасности и ключевым компонентом международных усилий России по киберпроблемам.[117] И это остается важным пунктом разногласий с США и с другими зрелыми демократиями.

На международной арене один из важных существующих договоров по кибербезопасности – это Конвенция по киберпреступности Совета Европы, так же из-

[112] «Доктрина информационной безопасности Российской Федерации», 9 сентября 2000; доступно на http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24b c32575d9002c442b!OpenDocument.

[113] Timothy Thomas, *Recasting the Red Star: Russia Forges Tradition and Technology Through Toughness* (Fort Leavenworth, KS: Foreign Military Studies Office, 2011), 137–52.

[114] Thomas, "Nation-State Cyber Strategies," 477–79.

[115] Hillary Clinton, "Remarks on Internet Freedom," 21 January 2010; доступно на www.state.gov/secretary/rm/2010/01/135519.htm

[116] Jason Healey, "Breakthrough or Just Broken? China and Russia's UNGA Proposal on Cyber Norms," *New Atlanticist* (21 September 2011); доступно на www.atlanticcouncil.org/blogs/new-atlanticist/breakthrough-or-just-broken-china-and-russia-s-unga-proposal-on-cyber-norms.

[117] Giles, "Russian Cyber Security," 2.

вестный как Будапештская конвенция, основное региональное соглашение, которое располагает потенциалом для того, чтобы его приняли и на глобальном уровне. Конвенция была подписана тридцатью девятью европейскими в основном странами – в том числе США, но не Россией, – с момента ее создания в 2001 году.[118] Этот договор дает схему сотрудничества между разными странами и частной индустрией в борьбе с киберпреступностью, предлагая модель, которую в потенциале можно будет распространить и на другие киберпроблемы.[119] Россия, однако, возражает против ратификации договора, считая, что он ущемляет ее суверенитет, так как в результате его применения могут появиться требования к российским властям сотрудничать при идентификации, к примеру, авторов кибератак в Эстонии в 2007 году, наряду с требованиями иностранных органов правопорядка о прекращении обширной киберпреступной деятельности, которая исходит с территории России.[120]

Вместо того чтобы поддерживать Будапештскую конвенцию, Россия подчеркивает необходимость нового международного режима, который в большей степени соответствовал бы ее точке зрения на кибербезопасность. Российские власти и российские ученые последовательно придерживаются позиции, что существующее международное право неадекватно и необходимы новые соглашения для укрепления национального суверенитета и сдерживания агрессивного поведения в киберпространстве.[121] Их предложения, в том числе и письмо к Генеральному секретарю ООН в соавторстве с Китаем, Таджикистаном и Узбекистаном, в целом направлено на достижение трех целей: ограничить инициативы США при разработке норм для киберпространства, которые они рассматривают как средство консолидирования конкурентных преимуществ США в киберпространстве; подтвердить права государств осуществлять мониторинг и контроль потока информации по Интернету, что для них важно для обеспечения внутренней безопасности и предотвратить дальнейшее развитие и распространение наступательных кибероружий. Эти принципы находятся в остром противоречии со значением, которое Запад придает свободному потоку информации, мерам по борьбе с киберпреступностью и ответственности государства за Интернет деятельность, которая осуществляется в рамках страны.[122] Эти различия на первый взгляд кажутся непреодолимыми, ограничивая шансы на достижение консенсуса по международному рамочному документу для кибероперациий.[123] Однако, по многим пунктам есть со-

[118] Council of Europe, "Convention on Cybercrime, Chart of Signatures and Ratifications," 22 March 2013; доступно на http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM =&DF=&CL=ENG.

[119] Hughes, "A Treaty for Cyberspace," 534.

[120] Giles, "'Information Troops'," 51; Giles, "Russia's Public Stance on Cyberspace Issues," 67.

[121] Dmitry I. Grigoriev, "Russian Priorities and Steps Towards Cybersecurity," in *Global Cyber Deterrence: Views of China, the U.S., Russia, India and Norway*, ed. Andrew Nagorski (New York: EastWest Institute, 2010).

[122] Carr, *Inside Cyber Warfare*, 34–35; Healey, "Breakthrough or Just Broken?"

[123] Shane Harris, "The Cyberwar Plan," *National Journal* (14 November 2009).

гласие, что дает хорошую отправную точку для сотрудничества – по обеспечению безопасности линий снабжения, по защите критической инфраструктуры, по предоставлению информации об угрозах и в борьбе с использованием Интернета с наркотрафикантами и педофилами.[124]

Хотя Россия может и подходит к кибербезопасности по-другому, чем США и их партнеры из НАТО, общие позиции, которые уже существуют, необходимо использовать во имя принятия более широкой повестки дня по кибербезопасности по всему спектру проблем безопасности, и в итоге и по другим темам, кроме как по безопасности. Расширение «диапазона сотрудничества» требует инновационного подхода к партнерству, ломку схем недоверия и создание новых средств нахождения и достижения общих целей.[125] В контексте отношений США-Россия и НАТО-Россия это будет означать не только преодоление недоверия к США и НАТО в России, но так же и сделать так, чтобы Россия чувствовала себя как равноправный партнер, наравне участвующий в выборе тем и принятии решений, какие бы формы взаимодействия при этом не использовались. Это потребует работы для преодоления как будто несовместимых взглядов на европейскую безопасность, различия стратегической культуры и традиции поразительного отсутствия устойчивого существенного сотрудничества.[126] Для достижения ощутимых результатов обе стороны должны иметь готовность пойти на некоторый риск как в смысле безопасности, так и в смысле внутренней политики.[127] Но такие риски будут скромной инвестицией, которая в потенциале может дать существенные прибыли по проблемам кибербезопасности, важные для всех затронутых сторон.[128]

Привлечение России к проблематике кибердомена

США и Россия давно заявили о своей взаимной заинтересованности в сотрудничестве по вопросам кибербезопасности, еще в 1998 году в декларации президента США Билла Клинтона и российского президента Бориса Ельцина, в которой стороны приняли на себя обязательство «сглаживать негативные аспекты революции в информационных технологиях», которые они охарактеризовали как «серьезный вызов» для безопасности обеих стран.[129] В том же заявлении подчеркивалась сов-

[124] Healey, "Breakthrough or Just Broken?"; "Russian Premier Chides USA over 'Unfair' Internet Policy, Urges 'Common Rules'," *Interfax* (30 October 2012); доступно на www.accessmylibrary.com/article-1G1-306951274/russian-premier-chides-usa.html.

[125] Martin E. Dempsey, "From the Chairman: Making Strategy Work," *Joint Forces Quarterly* 66 (2012): 2–3.

[126] James Sherr, "NATO and Russia: Doomed to Disappointment?" *NATO Review 2011*; доступно на www.nato.int/docu/review/2011/nato_russia/Disappointment/EN/index.htm.

[127] Oliker, et al., *Russian Foreign Policy*, 138.

[128] Dempsey, "From the Chairman: Making Strategy Work," 2–3.

[129] "Joint Statement on Common Security Challenges at the Threshold of the Twenty-First Century," 2 September 1998; доступно на http://www.gpo.gov/fdsys/pkg/WCPD-1998-09-07/pdf/WCPD-1998-09-07-Pg1696.pdf.

местная работа в ожидании Y2K,[130] которая выражалась в расширенной совместной подготовке и в мониторинге потенциальных технологических проблем при переходе в следующее тысячелетие.[131] С тех пор обе страны работали вместе в основном по таким вопросам, косвенно связанным с кибербезопасностью, как совместный мониторинг электронных процедур запуска баллистических ракет и модернизованных стандартов цифрового криптирования для горячей линии Белый дом – Кремль.[132] В декабре 2009 года на встрече комиссии ООН по разоружению и международной безопасности США и Россия подтвердили свою готовность к сотрудничеству, придя к соглашению укреплять безопасность Интернета и разработать нормы для военных операций в киберпростанстве.[133] Через короткое время это привело к резолюции Генеральной ассамблеи ООН, призывающей к «укреплению безопасности глобальных информационных и телекоммуникационных систем» и «изучению существующих и потенциальных угроз в сфере информационной безопасности и возможных коллективных мер для их предотвращения».[134] Единомыслие США и России по редакции резолюции – какими бы нечеткими и паллиативными не были формулировки – является прорывом в двусторонней кибердипломатии, который завершает десять лет предшествовавшего пустословного противоборства и открывает путь к дальнейшим официальным дискуссиям по вопросам кибербезопасности.[135]

Большинство последующих двусторонних консультаций преднамеренно проводились непублично и, по мнению вице-президента США Джозефа Байдена, были предназначены «для расширения сотрудничества и установления линий коммуникации на случай тревожных инцидентов».[136] Последняя серия переговоров, которые начались в феврале 2011 года, были сконцентрированы на таких областях взаимных интересов в сфере кибербезопасности, как обмен технической информацией об угрозах, работе по установлению общего понимания военных операций в киберпространстве и выработке протоколов коммуникации между

---

[130] Там же.

[131] Среди прочих, смотри к примеру, Stephen Barr, "U.S., Russia Agree to Establish Y2K Center," *Washington Post* (11 September 1999); Elizabeth Becker, "U.S. and Russia Agree on Joint Defense Against Y2K Debacles," *New York Times* (28 October 1999); Tom Bowman, "U.S., Russian Military Ally Against Y2K Bug," *Baltimore Sun* (27 October 1999); и Elizabeth Shogren, "U.S., Russia Cooperate on Y2K Concerns," *Los Angeles Times* (2 December 1999).

[132] Franz-Stefan Gady and Greg Austin, *Russia, the United States, and Cyber Diplomacy* (New York City: EastWest Institute, 2010), i.

[133] Там же.

[134] Объединенные нации, «Развитие в сфере информации и телекоммуникаций в контексте международной безопасности», Генеральная ассамблея ООН, A/Res/64/25 (2 декабря 2009).

[135] Gady and Austin, *Russia, the United States, and Cyber Diplomacy*, 3–4.

[136] Ellen Nakashima, "In U.S.-Russia Deal, Nuclear Communication System May Be Used for Cybersecurity," *Washington Post* (26 April 2012).

Москвой и Вашингтоном на случай связанных с кибербезопасностью кризисов.[137] Первым символическим жестом, направленным на создание взаимного доверия, стало то, что США согласились с предложением обменяться концептуальными документами по киберпространству, предоставив русским *Стратегию по операциям в киберпространстве* [138] Пентагона до того, как документ был официально опубликован в июле 2011 года.[139] Координатор США по кибербезопасности Хауард Шмидт и заместитель секретаря российского Совета по национальной безопасности Николай Климашин в июне 2011 года выступили с общим заявлением, в котором дискуссии были определены как «углубляющие взаимное понимание по вопросам национальной безопасности в киберпространстве»,[140] а позже Шмидт в своем блоге писал, что они являются «первым примером 'Перезагрузки' в отношениях США-Россия, открывающим путь к новому и важному измерению».[141]

Проводимые в течение более двух лет переговоры достигли кульминационной точки в двустороннем соглашении, заключение которого было объявлено президентом США Обамой и президентом России Путиным в июне 2013 года на саммите Г8 в Северной Ирландии. Как и ожидалось, совместное заявление, опубликованное Белым домом, дает описание мер, включающих обмен информацией между национальными группами реагирования на чрезвычайные ситуации в компьютерной сфере (ГРЧСКС), расширение ядерной горячей линии для обеспечения прямой коммуникации во время кризисов в киберсфере и учреждение рабочей группы по кибербезопасности в рамках двусторонней президентской комиссии США-Россия. Хотя в заявлении справедливо отмечено, что сотрудничество США и России по кибербезопасности «является существенным для защиты безопасности наших двух стран» и соглашение рассматривается как «знаменательный шаг», способствующий «реализации наших национальных и более общих международных интересов», остается сделать еще многое. Само желание сотрудничать говорит о важности кибербезопасности для обеих сторон – особенно в свете общей дискуссионности отношений США-Россия, – но этот договор следует рассматри-

[137] Howard Schmidt, "U.S. and Russia: Expanding the "Reset" to Cyberspace," The White House Blog (12 July 2011); доступно на http://www.whitehouse.gov/blog/2011/07/12/us-and-russia-expanding-reset-cyberspace. Смотри так же Barack Obama and Vladmir Putin, "Joint Statement by the Presidents of the United States of America and the Russian Federation on a New Field of Cooperation in Confidence Building," 17 June 2013; доступно на www.whitehouse.gov/the-press-office/2013/06/17/joint-statement-presidents-united-states-america-and-russian-federatio-0.

[138] United States Department of Defense, *Strategy for Operating in Cyberspace.*

[139] Nakashima, "In U.S.-Russia Deal."

[140] "Joint Statement by Cybersecurity Coordinator Schmidt and Deputy Secretary Klimashin: U.S. and Russian Delegations Meet to Discuss Confidence-Building Measures in Cyberspace," 23 June 2011; доступно на www.whitehouse.gov/sites/default/files/uploads/2011_klimashin_schmidt_cyber_joint_statement.pdf.

[141] Schmidt, "U.S. and Russia: Expanding the "Reset" to Cyberspace."

вать как осторожный, но необходимый первый шаг к углублению отношений, а не как конечный результат.[142]

До настоящего времени отношения между НАТО и Россией в сфере кибербезопасности были еще менее благоприятными. Переход от состояния противников времен Холодной войны к состоянию современных партнеров был неравномерным и все еще не завершен. В общем плане, отношения НАТО-Россия руководствуются Основополагающим актом о взаимных отношениях, сотрудничеству и безопасности между НАТО и Россией от 1997 года, который установил отношения на основе «НАТО+1», что означало, что по всем вопросам в двухсторонних отношениях с Россией НАТО будет выступать в качестве блока. В 2002 году эти отношения были актуализированы Римской декларацией, которая создала Совет НАТО-Россия (СНР) в качестве форума, на котором предполагалось, что Россия как равноправный партнер будет встречаться с государствами-членами для рассматривания вопросов, представляющих общий интерес.[143] С тех пор на СНР Россия неоднократно делала предварительные шаги для расширения сотрудничества по кибербезопасности, но НАТО никогда не демонстрировало достаточного желания – т.е. доверия, – чтобы ответить взаимностью. Во время встречи министров иностранных дел Совета НАТО-Россия в 2012 году самое категорическое решение, которое стороны оказались в состоянии принять, было то, что они «выразили заинтересованность в обмене мнениями по кибербезопасности и в обсуждении возможностей для военно-технического сотрудничества», что вряд ли можно назвать заявкой на настоящее сотрудничество.[144] Недавно на встрече министров иностранных дел в рамках Совета НАТО-Россия в апреле 2013 российский министр иностранных дел Сергей Лавров призвал к тому, чтобы Россия и НАТО работали вместе для укрепления кибербезопасности, и позднее заявил средствам массовой информации, что государственный секретарь США Джон Керри «незамедлительно поддержал» предложение, хотя никакого официального заявления со стороны США или НАТО по поводу предложения Лаврова не последовало.[145]

Как и при всех решениях Альянса, достичь единогласия между двадцатью восемью государствами-членами исключительно трудно. Любое взаимодействие с Россией является особым вызовом, имея в виду чувствительность нескольких ны-

[142] Obama and Putin, "Joint Statement by the Presidents of the United States and Russia."

[143] NATO–Russia Council, "About NRC," NATO-Russia Council Web Site (2013); доступно на www.nato-russia-council.info/en/about/.

[144] North Atlantic Treaty Organization, Press Release (2012) 053, "Meeting of the NATO-Russia Council at the Level of Foreign Ministers Held in Brussels on 19 April 2012," 19 April 2012; доступно на www.nato.int/cps/en/natolive/official_texts_86211.htm?mode=pressrelease.

[145] Сергей Лавров, «Речь и ответы на вопросы средств массовой информации российского министра иностранных дел Сергея Лаврова, подытожившего результаты сессии Совета НАТО-Россия на уровне министров иностранных дел, Брюссель, 23 апреля 2013, официальный сайт министерства иностранных дел Российской Федерации, 23 апреля 2013; доступно на www.mid.ru/BDOMP//brp_4.nsf/english/EFF6D7ADFD1A258B44257B58004CF50C.

нешних членов НАТО, которые раньше были членами Варшавского договора или бывшими советскими республиками и сейчас воспринимают свои отношения с Россией во времена Советского Союза через линзу доминирования или даже оккупации. Для них обсуждение партнерства с Россией граничит с ересью, и сотрудничество по кибербезопасности, особенно в свете кибератак на Эстонию в 2007 году и российско-грузинской войны в 2008 году, почти немыслимо. К счастью для своенравных членов НАТО – или, возможно более точно, потому что без их согласия никакие изменения невозможны, – политика НАТО по существу запрещает сотрудничество в сфере кибербезопасности с другими государствами вне Альянса, за исключением избранной группы самых близких партнеров, что требует изменения текущей политики или принятия исключений для каждого конкретного случая, с тем, чтобы осуществить какое бы то ни было реальное партнерство.[146]

Повестка дня для сотрудничества НАТО–Россия

Ввиду отсутствия какого бы то ни было сотрудничества в настоящее время между НАТО и Россией, список вопросов, который стал бы основой повестки дня для того, чтобы наконец-то НАТО привлекло Россию к сотрудничеству в сфере кибердомена, практически пуст – и НАТО должно четко заявить, что участие со стороны России является обязательным условием для того, чтобы двигаться вперед. Хотя Политика НАТО по кибероборонe признает, что НАТО будет «формировать свои международные ангажементы на основе общих ценностей и общих подходов»,[147] а в недавнем исследовании, проведенном НАТО, международные партнеры названы «важными акторами в кибероборонe НАТО», с которыми НАТО должно «развивать двусторонние отношения, … фокусируя усилия на обмене информации, на обмене лучших практик и на юридических соглашениях», паралич Альянса по этому вопросу мешает НАТО даже начать устанавливать отношения с Россией по вопросам взаимного интереса.[148] В результате члены НАТО, у которых имеются благоприятные двусторонние отношения с Российской Федерацией, обходят НАТО и работают напрямую с Россией по кибербезопасности и другим темам, что нейтрализует коллективное влияние НАТО и играет на руку стратегиче-

[146] Список программ партнерства НАТО разнообразен, и в теории, каждая страна-партнер имеет индивидуальный план сотрудничества и партнерства с НАТО, который может включать или не включать сотрудничество в сфере кибербезопасности. На деле, семь нечленов НАТО имеют весьма комплексные соглашения о сотрудничестве по кибербезопасности согласно Gerhard Jandl, "The Challenges of Cyber Security – A Government's Perspective," *Human Security Perspectives* (2012): 26–37. Для дополнительных подробностей по политике партнерства НАТО смотри North Atlantic Treaty Organization, "Partnership Tools"; доступно на www.nato.int/cps/en/natolive/topics_80925.htm.

[147] North Atlantic Treaty Organization, "Defending the Networks."

[148] Vincent Joubert, *Five Years after Estonia's Cyber Attacks: Lessons Learned for NATO*, NATO Defense College Research Paper No. 76 (Rome: Imprimerie Deltamedia Group, 2012), 7.

ской цели России маргинализовать НАТО всегда, когда это возможно.[149] Вместо того, чтобы сидеть на обочине в то время, как кибердомен развивается, сейчас у НАТО есть возможность и необходимость привести свои действия в соответствие со своей риторикой и принять реверансы России, направленные на сотрудничество по кибербезопасности. НАТО должно достичь внутреннего консенсуса по привлечению России относительно недорогостоящими, с невысоким уровнем риска мерами, с помощью которых обе стороны относительно легко могли бы добиться согласия в качестве первого шага к более существенному партнерству, при котором будут разрешены наиболее колючие проблемы, по которым позиции сторон существенно отличаются. Конкретно, НАТО должно стремиться к сотрудничеству с Россией для достижения следующих целей.

Создание Рабочей группы по кибербезопасности при Совете НАТО-Россия. Лучше всего было бы, если это будет отдельная рабочая группа наряду с рабочими группами по противоракетной обороне, логистике или терроризму. Если такой мандат покажется слишком широким для того, чтобы члены Альянса на него согласились, этот орган можно учредить в виде подгруппы в рамках Комиссии по науке для мира и безопасности с более узкой и более технической сферой компетенций. В любом случае, создание рабочей группы при СНР продемонстрирует намерение работать серьезно с Россией по кибербезопасности и обеспечить организационную форму для такого сотрудничества.[150]

Партнерские группы для реакции на случай чрезвычайных ситуаций, связанных с компьютерами. Вне зависимости от уровня доверия между НАТО и Российской федерацией, наличие установленных контактов между техническими экспертами, которые в состоянии реагировать в случаях кризисов, нельзя переоценить.[151] НАТО следовало бы коллективно принять прагматический подход некоторых из своих членов и начать серию ограниченных, технически ориентированных обменов между Техническим центром способностей для реагирования в случае инцидентов и российской ГРЧСКС для обмена технической информацией и определения, как лучшим образом осуществлять коммуникации в период кризисов.

Обмен разведывательной информацией, связанной с кибербезопасностью. Поскольку киберпространство постоянно развивается и злонамеренные акторы, которые в нем оперируют, непрерывно приспосабливаются, обеспечение актуальной

[149] Haider Ali Hussein Mullick, "Catching the BUG (Belarus, Ukraine and Georgia) – Russia's Buffer or NATO's Annex? A New Framework for Euro-Atlantic-Russian Cooperation," *Georgetown Journal of International Affairs* (4 May 2013); доступно на http://journal.georgetown.edu/2013/05/04/catching-the-bug-belarus-ukraine-and-georgia-russias-buffer-or-natos-annex-a-new-framework-for-euro-atlantic-russian-cooperation-by-haider-ali-hussein-mullick/.

[150] NATO-Russia Council, "About NRC."

[151] "Joint Statement on Bilateral Discussions on Cooperation in Cybersecurity, China Institute of International Relations (CICIR) – Center for Strategic and International Studies (CSIS)," Center for Strategic and International Studies (June 2012); доступно на http://csis.org/files/attachments/120615_JointStatement_CICIR.pdf.

информации о киберугрозах является постоянным вызовом. Так как обмен информацией даже в рамках НАТО может быть чувствительным и трудным процессом, тем более любое предложение обмениваться секретами с Россией на первый взгляд выглядит очень сомнительным – за исключением того, что во время своего визита в Москву в апреле 2013 года заместитель генерального секретаря НАТО Александр Вершбоу предложил создание двух центров, которые позволили бы России и НАТО обмениваться разведывательной информацией, вести совместное планирование и координировать операции по противоракетной обороне.[152] Хотя окончательное соглашение об учреждении этих двух центров далеко от завершения, и противоракетная оборона является не меньшим источником трений между США, НАТО и Россией, чем кибербезопасность, предложенные органы могли бы стать прототипом для клирингового дома для обмена информацией по киберугрозам, так же как и другой областью сотрудничества между НАТО и Россией. Такой клиринговый дом мог бы начать работу с небольших проектов и поначалу работать для совместного анализа прекрасных, но несекретных данных коммерческих фирм, занимающихся кибербезопасностью, и по мере укрепления доверия расширять свою деятельность в сторону более чувствительных и секретных разведывательных продуктов.[153]

Развитие мер по укреплению доверия. Организация по Безопасности и Сотрудничеству в Европе (ОБСЕ) почти заканчивает составление списка мер укрепления доверия (МУД), направленных на избежание недоразумений и предотвращения международных конфликтов между своими пятьюдесятью семью странами-участницами.[154] Хотя обнародованный проект списка мер свидетельствует об их несколько произвольном и не особо устойчивом характере,[155] соглашение, когда оно будет финализировано, станет важным началом диалога о кибербезопасности среди одной четверти государств мира и будет способствовать обмену информацией по терминологии кибербезопасности, доктрине и контактам между членами. НАТО должно основываться на повестке дня ОБСЕ для определения более де-

[152] Инна Соболева, «НАТО и Россия рассматривают возможность создания совместной противоракетной обороны», *Россия за заголовками* (8 апреля 2013); доступно на http://rbth.ru/politics/2013/04/08/nato_russia_consider_joint_missile-defense_system_24761.html.

[153] Mandiant Intel Team, "No Clearance Required: Using Commercial Threat Intelligence in the Federal Space," Mandiant Web Site (2 May 2013); доступно на www.mandiant.com/blog/clearance-required-commercial-threat-intelligence-federal-space/.

[154] Aliya Sternstein, "U.S., Russia, Other Nations Near Agreement on Cyber Early-Warning Pact," *Nextgov* (5 December 2012); доступно на www.nextgov.com/cybersecurity/2012/12/us-russia-other-nations-near-agreement-cyber-early-warning-pact/59977/.

[155] Jeffrey Carr, "OSCE's Cyber Security Confidence Building Measures Revealed by Anonymous," *Digital Dao* (13 November 2012); доступно на http://jeffreycarr.blogspot.de/2012/11/osces-cyber-security-confidence.html#!/2012/11/osces-cyber-security-confidence.html. Хакерская группа Анонимные украла с Интернет сервера ОБСЕ конфиденциальный проект МУД и предоставила документы онлайн. Блог Карра дает резюме и анализ содержания, наряду со ссылкой на украденные документы.

тального и более амбициозного набора МУД с Россией, в том числе механизмов раннего предупреждения, обмена техническими рекомендациями по кибербезопасности и усовершенствованию коммуникационных каналов на случай киберкризисов.[156] Имея в виду, что все двадцать восемь стран НАТО и Россия являются членами ОБСЕ, достижение консенсуса по мерам укрепления доверия в СНР будет возможным, но надо пройти долгий путь преодоления почти парализующего опасения России оказаться обвиненной в киберинциденте, в котором она юридически не играла никакой роли.[157] И поскольку НАТО и Россия имеют длинный послужной список разработки МУД в отношении ядерных вооружений, адаптирование существующих процедур и процессов к кибербезопасности выглядит непосредственно достижимым.

Проведение совместных учений по кибероборонe. Опасения относительно того, позволять ли России участвовать в киберучениях, многочисленны – как возражения против какой бы то ни было роли России, так и опасения, что Россия будет давить на других участников учений, в частности стран на постсоветском пространстве, – но НАТО успешно работало с Москвой в некиберконтексте многие годы. НАТО следовало бы принять похожий подход к кибербезопасности. С 2010 года Европейское командование вооруженных сил США (EUCOM) проводит серию оборонных киберучений «Кибер усилие», в рамках и одновременно с более масштабным учением по отработке вопросов командования и управления «Совместное усилие».[158] Поскольку командующий EUCOM является и Верховным главнокомандующим объединенными вооруженными силами НАТО, это позволяет принимать участие в учении всем странам НАТО, а так же и другим странам, участие которых не предполагается Политикой НАТО по сотрудничеству в области кибербезопасности, таким образом на практике выходя за рамки руководящих документов НАТО и расширяя круг разрешенных участников. В 2012 году в учении принимали участие 175 сотрудников из тридцати двух стран, некоторые из которых являются членами НАТО, а другие нет, и акцент ставился на процедуры защиты компьютерных сетей и реакцию в случаях киберинцидентов.[159] НАТО следовало бы использовать этот форум для привлечения России, пригласив ее для

[156] Detlev Wolter, "Looking towards the Future of Cyber Security: What Does a Stable Cyber Environment Look Like?" Speech at the UNIDIR Cyber Security Conference 2012 (8 November 2012); доступно на www.unidir.ch/files/conferences/pdfs/pdf-conf1920.pdf.

[157] Эта ситуация, обычно обозначаемая как «фальшивый флаг», описана в ряде источников, в том числе и в Geers, *Strategic Cyber Security*, 118; и Nye, *Cyber Power*, 16–17. Это было и основной темой почти каждого российского оратора на 7-ом Международном форуме по сотрудничеству государственных властей, гражданского общества и бизнес сообщества в сфере обеспечения международной информационной безопасности, состоявшемся 22-25 апреля в Гармиш-Партенкирхене, Германия.

[158] "Exercise Combined Endeavor."

[159] James G. Stavridis, Testimony before the 113th Congress, House and Senate Armed Services Committee Testimony, 19 March 2013; доступно на www.armed-services.senate.gov/statemnt/2013/03%20March/Stavridis%2003-19-13.pdf, 13.

участия в будущих изданиях этого учения, сначала в качестве наблюдателя, а затем полноправного участника, подобно тому как это делалось в последние годы в отношении некиберучений.[160]

Также НАТО через Совместный центр повышения компетенций в сфере кибербороны (СЦПККО) в Таллинне, Эстония, проводит серию ежегодных более ограниченных учений по техническим аспектам киберобороны, называемых «Сомкнутые щиты». В учении в 2013 году принимали участие ГРЧСКС из штаб-квартиры НАТО, восьми стран-членов НАТО и из Финляндии (одна из стран, для которых Политика НАТО по безопасности разрешает партнерство по вопросам кибербезопасности), которые в реальном времени обеспечивали защиту компьютерных сетей от широкомасштабных кибератак.[161] Хотя текущая политика по безопасности запрещает российское участие, руководящей комиссии СЦПККО следовало бы попросить заинтересованные стороны об явном разрешении привлечь Россию для участия в учениях «Сомкнутые щиты», сначала в качестве наблюдателя, а затем участника, возможно в партнерстве с другой ГРЧСКС.

Достичь консенсуса по международному киберправу. Фундаментальные разногласия относительно адекватности существующего международного права – США и НАТО хотят применять существующее международное право к киберпроблемам, тогда как Россия настаивает, что необходимы новые международные соглашения – существенно замедляют прогресс по другим киберпроблемам, поскольку право определяет, что разрешено и что не разрешено в киберпространстве. В качестве первого шага к разрешению этих разногласий НАТО следует привлечь Россию к своим усилиям по интерпретации и развитию международного закона по киберпроблематике, что способствовало бы смягчению разделения, существующего между двумя лагерями.

Одним легким, с невысокой степенью риска, первым шагом было бы пригласить участников из России на проводимый дважды в году Курс по международному праву по кибероперациям, организуемый СЦПККО, колледжем военно-морских сил США и Школой НАТО. Курс предназначен для юридических советников органов, формирующих политику в области киберпространства, и он дает основные знания по международному праву, относящиеся к кибероперациям. Этот курс мог бы стать хорошим форумом для вдумчивого взаимодействия между юридическими экспертами из НАТО и России.[162]

НАТО следует признать пропущенную возможность, когда оно спонсировало разработку «Таллиннского руководства» практически без представительства или

---

[160] James G. Stavridis, Testimony before the 112th Congress, House and Senate Armed Services Committee Testimony, 20 March 2011; доступно на www.armed-services.senate.gov/statemnt/2011/03%20March/ Stavridis%2003-29-11.pdf, 17.

[161] CCD COE, "NATO Team Wins the Locked Shields Cyber Defence Exercise," NATO Cooperative Cyber Defense Centre of Excellence Web Site (26 April 2013); доступно на www.ccdcoe.org/413.html.

[162] CCD COE, "International Law of Cyber Operations," NATO Cooperative Cyber Defense Centre of Excellence Web Site; доступно на www.ccdcoe.org/352.html.

учета мнения экспертов из России и практически из никаких других стран, кроме как из Западной Европы и Северной Америки, что привело к использованию юридических оснований, которые по существу уже проповедуются приверженцами идеи международного киберправа. В результате Россия заняла позицию или игнорировать, или отвергать (в зависимости от источника) толкования международного права, представленные в «Таллиннском руководстве».[163] Будущие проекты такого характера важны, но их влияние будет оставаться ограниченным, если состав контрибуторов будет исключать потенциальных участников, как то предполагается планом последующего проекта Таллинн 2.0 рассмотрения международного права применительно к кибератакам, которые остаются ниже порога вооруженного нападения.[164] Действительно, найти российского юридического эксперта с соответствующими правомочиями, который был бы конструктивным участником, а не препятствием для достижения прогресса, может оказаться трудной задачей. Однако, когда альтернативой является создание еще одного справочного пособия, которое «одна большая часть мира не будет считать … легитимным»,[165] НАТО следует спонсировать проекты с более всеохватным кругом участников, которые с большей вероятностью будут широко приняты и будут уменьшать различия между противоположными точками зрения на ключевые проблемы международного киберправа.

Взаимодействие США-Россия в сфере кибербезопасности

Тогда как между НАТО и Россией сотрудничества по киберпроблематике практически не существует, двустороннее киберсотрудничество между США и Россией можно определить как находящееся в фазе зарождения и пока весьма осторожное, даже если рассматривать в самом оптимистическом свете прорывное соглашение по кибербезопасности от июня 2013 года. Хотя *Международная стратегия для киберпространства* США от 2011 года призывает к «двусторонним диалогам в широком спектре» для «стимулирования общих действий против новых вызовов в киберпространстве»,[166] существует очень мало публичной информации о работе с Россией по каким-либо проблемам кибербезопасности, кроме эпизодических от-

[163] "The Applicability of International Law in Cyberspace – From If to How?" Panel Three at the Georgetown University Conference on the International Law on Cyber (10 April 2013); доступно на http://lsgs.georgetown.edu/events/InternationalEngagementonCyber2013/PanelThreeApplicabilityofInternationalLawinCyberspace041013.pdf. Комментарии доктора Анатолия Стрельцова из Московского государственного университета имени М.В. Ломоносова в этой стенограмме являются репрезентативными.

[164] CCD COE, "Four Legal Experts Appointed as Centre's Senior Fellows," NATO Cooperative Cyber Defense Centre of Excellence Web Site (9 May 2013); доступно на www.ccdcoe.org/422.html.

[165] "Apply International Law to Cyber-Warfare? Good Luck," *The Economist* (23 March 2013).

[166] Office of the President of the United States, *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World* (Washington, D.C.: Government Printing Office, 2011), 12.

четов в средствах массовой информации о содействии правоохранительных органов в разоблачении мошеннических групп в Интернете.[167] С соглашения от июня 2013 года мог бы начаться новый этап сотрудничества между США и Россией по киберпроблемам, но скромные меры, которые в нем содержались, являлись скорее символическими шагами, свидетельствующими о желании работать вместе, чем серьезными решениями наиболее наболевших проблем кибербезопасности, с которыми сталкиваются оба государства. Учреждение рабочей группы по киберпроблематике под эгидой Президентской комиссии США-Россия предоставило форум, с помощью которого обе стороны могли бы поддерживать импульс начавшегося сотрудничества. США и России следует развивать достигнутый в последнее время успех для упрочнения их отношений в киберпространстве путем осуществления следующих шагов.

Укрепление партнерства ГРЧСКС. Какое бы развитие взаимодействия между российскими и американскими ГРЧСКС не происходило после совместного заявления Обамы и Путина о сотрудничестве по кибербезопасности, все случалось за закрытыми дверями, – и почти наверняка этого было недостаточно. Что касается партнерства между российскими и американскими ГРЧСКС, значение того факта, чтобы знать, кому позвонить в случае кризиса, неизмеримо, и увеличение частоты взаимодействия между ГРЧСКС США и России практически не имеет отрицательных сторон. Со временем обе стороны должны будут начать стремиться к расширенному сотрудничеству в реальном времени между техническими экспертами и аналитиками, к совместной технической подготовке и обмену персоналом, к обмену информацией об угрозах и тенденциях, к развитию стандартизированных процедур менеджмента инцидентов для укрепления доверия между двумя командами и для расширения оперативной совместимости во время кризисов.

Проведение совместных учений по кибероборонe. США следует пригласить Россию, чтобы она начала принимать участие в его учениях «Кибер усилие», руководимых Европейским командованием, что важно, как для прямого взаимодействия с Россией, так и для форсирования привлечения России к сотрудничеству с НАТО в сфере кибероборонbы. В то же время Тихоокеанское командование США (PACOM) также ежегодно проводит свое учение «Кибер усилие», в котором в 2012 году участвовали двадцать два государства из Азиатско-Тихоокеанского региона.[168] Поскольку никто из участников учений PACOM не является бывшей советской республикой или членом Варшавского Договора, участие России, возможно, вызовет меньше противоречий, чем на европейском театре. США следует пригласить Российскую Федерацию принять участие в обоих учениях «Кибер уси-

[167] Nikola Krastev, "In U.S. Cybercrime Case, Track Record Indicates Russia Willing to Cooperate," *Radio Free Europe/Radio Liberty* (9 October 2010); доступно на http://www.rferl.org/content/In_US_Cybercrime_Case_Track_Record_Indicates_Russia_Willing_To_Cooperate/2185564.html.

[168] Carl Hudson, "Pacific Endeavor 2012 Begins," United States Pacific Command Web Site (8 August 2012); доступно на www.pacom.mil/media/news/2012/08/08-pacific-endeavor-2012-begins.shtml.

лие», сначала в качестве наблюдателя, с намерением дойти до полноправного участия как можно скорее. Надо работать для включения аспектов кибероборонны в текущие совместные американо-российские учения – «Северный орел», «Атлас вижэн», «Бдительный орел» – с целью улучшить оперативную совместимость в сфере кибероборонны между вооруженными силами на всех уровнях.[169]

Сотрудничество в борьбе с киберпреступлениями. Сотрудничество США-Россия в борьбе с киберпреступностью до сих пор было эпизодическим, хотя рост организованных русских преступных киберсетей в последние годы не замедлялся, составляя в 2011 году 36 процентов от мировой киберпреступности, несмотря на декларированные российскими властями попытки справиться с ними.[170] Для США идеальным выходом было бы убедить Россию принять Будапештскую конвенцию, что, однако, маловероятно, имея в виду упорное сопротивление России на основании суверенности. США следует продолжать давление на Россию, направленное на принятие Будапештской конвенции, но и не отказываться от работы по улучшению сотрудничества с Россией в борьбе с киберпреступностью через Римо-Лионскую Подгруппу по высокотехнологическим преступлениям Г8, которая создала небольшую, но важную программу по сотрудничеству в области охраны правопорядка.[171] США следует поощрять включение России в программы противодействия таким типам онлайн преступлениям, для борьбы с которыми Россия публично призывает к расширенному сотрудничеству, и чье содержание не вызывает разногласий, например, борьба с детской порнографией или с трафиком наркотиков.[172] Еще более прямолинейно США следует работать на укрепление двустороннего сотрудничества в сфере правопорядка по киберпроблемам, используя реализованный недавно прогресс после взрывов во время Бостонского марафона,[173] с тем, чтобы упрочить отношения и улучшить взаимодействие между обеими сто-

---

[169] Gerald O'Dwyer, "Norway Hails Northern Eagle as Bridge-Builder," *DefenseNews* (24 August 2012); доступно на www.defensenews.com/article/20120824/DEFREG01/308240002/Norway-Hails-Northern-Eagle-Bridge-builder. Смотри так же "Military Cooperation: Past Events," U.S. Department of State Web Site; доступно на http://m.state.gov/mc38712.htm.

[170] Loek Essers, "Russian Cybercriminals Earned $4.5 Billion in 2011," *ComputerWorld* (24 April 2012); доступно на http://www.computerworld.com/s/article/9226498/Russian_cybercriminals_earned_4.5_billion_in_2011.

[171] "The G8 24/7 Network of Contact Points Protocol Statement," December 2007; доступно на www.oas.org/juridico/english/cyb_pry_G8_network.pdf.

[172] ТАСС, «Россия призывает к сотрудничеству в борьбе с детской порнографией», *радио Голос России* (1 июня 2012); доступно на http://english.ruvr.ru/2012_06_01/76693555/. К примеру, несмотря на публичные заявления, Россия не одна из сорока девяти стран, которы создали *Глобальный альянс против сексуального насилия над детьми* в декабре 2012. Смотри так же United States Department of Justice. "Attorney General Eric Holder and High-Level Officials Launch Global Alliance against Child Sexual Abuse Online," Department of Justice Web Site (4 December 2012); доступно на www.justice.gov/opa/pr/2012/December/12-ag-1438.html.

[173] Ellen Barry, "After Boston Bombing, American Ties with Russia Improve," *New York Times* (29 April 2013).

ронами в практической реализации Договора о взаимном оказании правовой помощи.[174] Улучшение координации следует воспринимать не как нечто само собой разумеющееся, несмотря на недавнюю оттепель, а как тесное окно, которое открылось для США, чтобы дополнить их обычные усилия оказывать давление на Россию по теме киберпреступности способом, который способствовал бы разрешению критических проблем, связанных с организованной преступностью.

Принятие общих стандартов для инфраструктуры с открытыми ключами. Инфраструктура с открытыми ключами (ИОК) является технической концепцией, которая использует «цифровую электронную подпись» для верификации интегритета данных и идентичность отправителя при обмене электронной информацией. В докладе от 2008 года, подготовленного для избранного тогда президента Обамы, предупреждалось, что «Создание возможности иметь надежную информацию о том, кто или какое устройство посылает конкретный пакет данных в киберпространстве, должно быть обязательной частью любой эффективной стратегии кибербезопасности».[175] Технология ИОК является важным средством обеспечения такой уверенности. Ее применение Министерством обороны США посредством регистрации с помощью карт общего доступа (КОД) привело к 50 процентному уменьшению частоты кибератак через год после введения этой технологии.[176] В своей *Национальной стратегии для доверительной идентификации в киберпространстве* от 2011 года[177] США обязались работать по этому вопросу с другими странами, но показывают определенные колебания при принятии увертюр России к сотрудничеству из-за опасений, что Россия попытается контролировать Интернет-содержание и ограничивать использование его диссидентами.[178] Несмотря на это, технической группе следует провести совместное исследование требований и стандартов с непосредственной целью разработать общие для США и России ИОК стандарты таким образом, чтобы был обеспечен баланс между требованиями безопасности и гражданскими свободами.[179] Двустороннее соглашение о таких стандартах – а точнее, соглашение, которое было бы совместимым с другими уже существующими соглашениями, – стало бы краеугольным камнем на пути к более широкому, многостороннему консенсусу по менеджменту электронной идентич-

[174] *Mutual Legal Assistance Treaty between the United States of America and the Russian Federation* (17 June 1999); доступно на www.state.gov/documents/organization/123676.pdf.

[175] Center for Strategic and International Studies, *Securing Cyberspace for the 44th Presidency. Report of the CSIS Commission on Cybersecurity for the 44th Presidency* (Washington, D.C.: Center for Strategic and International Studies, 2008), 62.

[176] Там же.

[177] Office of the President of the United States, *National Strategy for Trusted Identities in Cyberspace* (Washington, D.C.: Government Printing Office, 2011), 4.

[178] John Markoff and Andrew E. Kramer, "U.S. and Russia Differ on a Treaty for Cyberspace," *New York Times* (28 June 2009).

[179] Gady and Austin, *Russia, the United States, and Cyber Diplomacy*, 9–12.

ности.[180] Последующие усилия могли бы быть сосредоточены на создании инфраструктуры и стимулов для американского и российского частных секторов в начале сотрудничества в сфере будущих ИОК стандартов и выработки рекомендаций к политике в киберпространстве.[181] Все эти меры помогли бы заняться проблемами озабоченности США по поводу киберпреступности, тревогами России об атаках типа «фальшивый флаг» и общими проблемами защиты критической инфраструктуры от киберугроз.

Достижение консенсуса по международному праву для киберпространства. Из-за разногласий между США и Российской Федерацией и их союзников по основному вопросу об адекватности существующего международного права в отношении проблем кибербезопасности, движение к глобальному консенсусу по этим важным темам было медленным и неравномерным. Хотя Россия давно настаивает на подготовке глобального договора для регулирования киберпространства, отсутствие широкой международной поддержки делает такое соглашение очень маловероятным. Тем не менее, согласие относительно норм поведения в киберпространстве необходимо, и что важно – достижимо и без комплексного международного юридического соглашения. Наоборот, мозаика из двусторонних или более ограниченных многосторонних договоренностей, у которых есть общие моменты, с течением времени приведет к достижению согласия по наиболее общим принципам. Хотя США и Россия придерживаются противоположных точек зрения по многим проблемам, по некоторым важным вопросам у них похожие позиции. К примеру, в российском документе по военным операциям в киберпространстве от 2011 года высказывается согласие, что принципы международного гуманитарного права о недопустимости дискриминации, использовании защитных индикаторов и запрета на измену применимы к киберпространству.[182] Хотя это согласие не является чем-то революционным, оно показывает, что есть области, в которых интересы США и России пересекаются, и они могут стать отправной точкой для программы взаимодействия. Это работа, которую Институт Восток-Запад уже начал по Дорожке 2 дипломатической инициативы, направленной на изучение вопроса, как обращаться с «критической гуманитарной инфраструктурой» и как применять «важные эмблематические женевские концепции» (как Красный крест или Красный полумесяц) в киберпространстве.[183] Такие усилия надо поощрять и поддержи-

[180] Смотри Combined Communications-Electronics Board, "PKI Cross-Certification Between CCEB Nations" (30 July 2007) как пример ИОК стандартов для Австралии, Канады, Новой Зенландии, Объединенного Королевства и Соединенных Штатов. Доступно на http://info.publicintelligence.net/CCEB-PKI.pdf.

[181] Gady and Austin, *Russia, the United States, and Cyber Diplomacy*, 11.

[182] Министерство обороны Росссийской Федерации, «Концептуальные взгляды на деятельность Вооруженных сил Российской Федерации в информационном пространстве».

[183] Karl Frederick Rauscher and Valery Yashchenko, eds., *Russia–U.S. Bilateral on Cyber Security: Critical Terminology Foundations* 1 (New York and Moscow: EastWest Institute and Moscow State University, April 2011), 7; доступно на www.ewi.info/system/files/reports/Russia-U%20S%20%20bilateral%20on%20terminology%20v76%20%282%29.pdf.

вать, и когда они достигнут определенной степени зрелости, переводить в дипломатические каналы для кодификации – по существу, добавляя кусочек к кусочку к мозаике обычного международного права, которого должно быть достаточно для нужд практики при отсутствии комплексного международного договора.

Заключение

Отношения между Соединенными Штатами и Россией и между НАТО и Россией – дело трудное, запутанное, с эпизодическими подъемами, прерывающими долгие периоды некомфортного сосуществования, периоды сварливости и перемежающейся необузданной раздражительности. Политические проблемы, которые держат обе стороны в натянутых отношениях, похоже, постоянно возникают снова и снова, и на месте каждой разрешенной проблемы почти сразу же появляется другая, похоже неразрешимая, дилемма. В этих отношениях мало взаимного доверия, наряду с ощущением Россией недостатка взаимного уважения и равенства, которое негативно окрашивает все взаимодействия с другой стороной. Несмотря на эти проблемы, Россия, НАТО и США имеют сильно взаимозависимые отношения в политическом, дипломатическом, военном, экономическом плане, как и во многих других важных измерениях. Короче, они нужны друг другу, в частности, чтобы справиться с множеством ключевых вызовов в текущей международной среде, большая часть которых требует региональной и даже глобальной реакции. Одной такой проблемой является кибербезопасность, сфера, в которой все три стороны находятся в числе лидеров в смысле возможностей, но в которой противоречивое понимание природы киберпространства и его использования мешают им собраться вместе для разрешения проблем, созданных киберреальностью. Хотя прогресс не может быть легкодостижимым, интересы США, НАТО и России пересекаются в нескольких ключевых областях, таких как технические возможности и развитие стандартов, предоставление разведывательной информации об угрозах, усиление интероперабельности и достижение консенсуса по созданию международного права – области, пригодные для дальнейшего изучения на предмет сотрудничества. Принимая ограниченные и обдуманные риски с целью следовать этой повестке дня, все стороны могут выиграть, начальные успехи по этим вопросам создадут условия для дальнейшего сотрудничества по кибербезопасности, и возможно, помогут перейти к сотрудничеству по более широкому спектру проблем по мере укрепления доверия и навыков взаимодействия.

Литература

"Apply International Law to Cyber-Warfare? Good Luck." *The Economist* (2013).

2012 Norton Cybercrime Report. Symantec, 2012.

About NRC. NATO-Russia Council Web Site, 2013.

Active Engagement, Modern Defence. Lisbon Summit, 2010.

Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization. Brussels: NATO, 2010.

Alexander, Keith. *U.S. Cybersecurity Policy and the Role of U.S. CYBERCOM* In *CSIS Cybersecurity Policy Debate Series*., 2010.

Angell, Norman. *The Great Illusion: A Study of the Relation of Military Power in Nations to Their Economic and Social Advantage*. New York: Putnam, 1910.

Barr, Stephen. "U.S., Russia Agree to Establish Y2K Center." *Washington Post* (1999).

Barry, Ellen. "After Boston Bombing, American Ties with Russia Improve." *New York Times* (2013).

Becker, Elizabeth. "U.S. and Russia Agree on Joint Defense Against Y2K Debacles." *New York Times* (1999).

Betz, David J., and Tim Stevens. *Cyberspace and the State: Toward a Strategy for Cyber-Power*. New York: Routledge, 2011.

Beyrle, John. *Priorities for Russia-U.S. Relations: A Statement by Former Ambassadors to Washington and Moscow*. Carnegie Endowment for International Peace Web Site, 2013.

Blank, Stephen J.. "*Introduction*." In *Prospects for U.S.-Russian Security Cooperation*, 1. Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 2009.

Boudreaux, Benjamin. "Cyber Diplomats." *State Magazine* (2013): 32.

Bowman, Tom. "U.S., Russian Military Ally Against Y2K Bug." *Baltimore Sun* (1999).

Carr, Jeffrey. *Inside Cyber Warfare*. Sebastopol, CA: O'Reilly Media, 2010.

Carr, Jeffrey. *OSCE's Cyber Security Confidence Building Measures Revealed by Anonymous*. Digital Dao, 2012.

Carr, Jeffrey. *The Myth of the CIA and the Trans-Siberian Pipeline Explosion*. Digital Dao, 2012.

Churchill, Winston. "The War Memoirs of Winston Churchill." *Life Magazine* (1948): 63.

Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Harper Collins, 2010.

Clarke, Richard A.. *War from Cyberspace* In *The National Interest*., 2009.

Clinton, Hillary. *Remarks on Internet Freedom*., 2010.

Coalson, Robert. *Former U.S. State Dep't Official Pifer Asks, 'Are the Russians Ready to Reengage?'*. Radio Free Europe/Radio Liberty, 2012.

Comprehensive National Cybersecurity Initiative. Washington, D.C.: The White House, 2009.

Concept of the Foreign Policy of the Russian Federation. Ministry of Foreign Affairs of the Russian Federation, 2013.

Convention on Cybercrime, Chart of Signatures and Ratifications. Council of Europe, 2013.

Cutts, Andrew. "*Warfare and the Continuum of Cyber Risks: A Policy Perspective*." In *The Virtual Battlefield: Perspectives on Cyber Warfare*, 69. Amsterdam: IOS Press, 2009.

Dempsey, Martin E.. "From the Chairman: Making Strategy Work." *Joint Forces Quarterly* 66 (2012): 2-3.

Developments in the Field of Information and Telecommunications in the Context of International Security. United Nations General Assembly, 2009.

Dictionary of Military and Associated Terms In *Joint Publication*. Vol. 1-02. Washington, D.C.: United States Department of Defense, Government Printing Office, 2011.

Dion, Maeve. "*Different Legal Constructs for State Responsibility*." In *International Cyber Security Legal & Policy Proceedings 2010*, 69. Tallinn, Estonia: Cooperative Cyber Defence Center of Excellence, 2010.

Essers, Loek. *Russian Cybercriminals Earned $4.5 Billion in 2011*. ComputerWorld, 2012.

Fallows, James. *Cyber Warriors*. The Atlantic, 2010.

Flook, Kara. *Russia and the Cyber Threat*. American Enterprise Institute Critical Threats, 2009.

Four Legal Experts Appointed as Centre's Senior Fellows. NATO Cooperative Cyber Defense Centre of Excellence Web Site, 2013.

Fulghum, David A.. "China Cyber-skills Are Improving But Still Don't Top Russia and Israel." *Aviation Week* (2012).

Gady, Franz-Stefan, and Greg Austin. *Russia, the United States, and Cyber Diplomacy*. New York City: EastWest Institute, 2010.

Gearan, Anne. "Sour U.S.-Russia Relations Threaten Obama's Foreign Policy Agenda." *Washington Post* (2013).

Geers, Kenneth. "Cyberspace and the Changing Nature of Warfare." *SC Magazine* (2008).

Geers, Kenneth. *Strategic Cyber Security*. Tallinn, Estonia: Cooperative Cyber Defence Center of Excellence, 2011.

Giles, Keir. "*'Information Troops'—A Russian Cyber Command?*" In *3rd International Conference on Cyber Conflict*, 50. Tallinn: CCD COE Publications, 2011.

Goodman, Will. "Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly* 4, no. 3 (2010): 102-35.

Graham, Thomas E., and Dmitri Trenin. "Why the Reset Should Be Reset." *New York Times* (2012).

Greenberg, Andy. *McAfee Explains the Dubious Math behind Its 'Unscientific' $1 Trillion Data Loss Claim*. Forbes, 2012.

Greene, Samuel A., and Dmitri Trenin. *(Re) Engaging Russia in an Era of Uncertainty* In *Policy Brief*. Washington, D.C.: Carnegie Endowment for International Peace, 2009.

Grigoriev, Dmitry I.. "*Russian Priorities and Steps Towards Cybersecurity*." In *Global Cyber Deterrence: Views of China, the U.S., Russia, India and Norway*. New York: EastWest Institute, 2010.

Harris, Shane. "The Cyberwar Plan." *National Journal* (2009).

Häußler, Ulf. "*Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO Treaty*." In *International Cyber Security Legal & Policy Proceedings 2010*, 104-5. Tallinn, Estonia: Cooperative Cyber Defence Center of Excellence, 2010.

Healey, Jason. *Breakthrough or Just Broken? China and Russia's UNGA Proposal on Cyber Norms*. New Atlanticist.

Healey, Jason. *Comparing Norms for National Conduct in Cyberspace*. New Atlanticist, 2011.

Hudson, Carl. *Pacific Endeavor 2012 Begins*. United States Pacific Command Web Site, 2012.

Hughes, Rex. "A Treaty for Cyberspace." *International Affairs* 86, no. 2 (2010): 533.

International Law of Cyber Operations. NATO Cooperative Cyber Defense Centre of Excellence Web Site, 2013.

International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World. Washington, D.C.: Government Printing Office, 2011.

Joint Statement by Cybersecurity Coordinator Schmidt and Deputy Secretary Klimashin: U.S. and Russian Delegations Meet to Discuss Confidence-Building Measures in Cyberspace., 2011.

Joint Statement on Bilateral Discussions on Cooperation in Cybersecurity, China Institute of International Relations (CICIR)–Center for Strategic and International Studies (CSIS). Center for Strategic and International Studies, 2012.

Joint Statement on Common Security Challenges at the Threshold of the Twenty-First Century., 1998.

Joubert, Vincent. *Five Years after Estonia's Cyber Attacks: Lessons Learned for NATO* In *NATO Defense College, Research Paper*. Rome: Imprimerie Deltamedia Group, 2012.

Keohane, Robert O., and Joseph S. Nye. *Power and Interdependence*. Vol. 3rd ed. New York: Longman, 2001.

Kramer, David J.. *The Russia Challenge: Prospects for US-Russian Relations* In *Policy Brief*. Washington, D.C.: The German Marshall Fund, 2009.

Kramer, Franklin D.. "*Cyberpower and National Security: Policy Recommendations for a Strategic Framework*." In *Cyberpower and National Security*, 12. Washington, D.C.: National Defense University Press, 2009.

Krastev, Nikola. *In U.S. Cybercrime Case, Track Record Indicates Russia Willing to Cooperate*. Radio Free Europe/Radio Liberty, 2010.

Kuehl, Daniel T.. "*From Cyberspace to Cyberpower: Defining the Problem*." In *Cyberpower and National Security*. Washington, D.C.: National Defense University Press, 2009.

Lavrov, Sergey. *Speech of and Answers to Questions of Mass Media by Russian Foreign Minister Sergey Lavrov Summarizing the Results of the Session of NATO-Russia Council at the Foreign Minister Level*. Brussels, 2013.

Lewis, James. "Five Myths about Chinese Hackers." *Washington Post* (2013).

Libicki, Martin. *Cyberdeterrence and Cyberwarfare*. Santa Monica, CA: RAND, 2009.

Linkevicius, Linas. "Reset with Russia, but with Reassurance." *International Herald Tribune*.

Markoff, John, and Andrew E. Kramer. "U.S. and Russia Differ on a Treaty for Cyberspace." *New York Times* (2009).

Masters, Greg. "Global Cybercrime Treaty Rejected at U.N." *SCMagazine* (2010).

Mazanec, Brian M.. "The Art of (Cyber) War." *Journal of International Security Affairs* (2009).

McGee, Joshua. *US-Russia Diplomacy -The "Reset" of Relations in Cyberspace*. Center for Strategic and International Studies Web Site, 2011.

Measuring the Information Society 2012 . Geneva: International Telecommunications Union, 2012.

Mullick, Haider Ali Hussei. "Catching the BUG (Belarus, Ukraine and Georgia)-Russia's Buffer or NATO's Annex? A New Framework for Euro-Atlantic-Russian Cooperation." *Georgetown Journal of International Affairs* (2013).

Mulvenon, James C., and Gregory J. Rattray. *Addressing Cyber Instability: Executive Summary*. Cyber Conflict Studies Association Web Site, 2012.

Mutual Legal Assistance Treaty between the United States of America and the Russian Federation., 1999.

Nakashima, Ellen. "In U.S.-Russia Deal, Nuclear Communication System May Be Used for Cybersecurity." *Washington Post* (2012).

National Strategy for Trusted Identities in Cyberspace. Washington, D.C.: Government Printing Office, 2011.

NATO Team Wins the Locked Shields Cyber Defence Exercise. NATO Cooperative Cyber Defense Centre of Excellence Web Site, 2013.

No Clearance Required: Using Commercial Threat Intelligence in the Federal Space. Mandiant Web Site, 2013.

Nye, Joseph S.. "*Independence and Interdependence*." In *Power in the Global Information Age*, 154. New York: Routledge, 2004.

Nye, Joseph S.. "*The Information Revolution and American Soft Power*." In *Power in the Global Information Age*, 81-82. New York: Routledge, 2004.

Nye, Joseph S.. *Cyber Power*. Cambridge, MA: Belfer Center for Science and International Affairs, 2010.

Nye, Joseph S.. *Understanding International Conflicts*. Vol. 4th ed. New York: Longman, 2003.

O'Dwyer, Gerald. *Norway Hails Northern Eagle as Bridge-Builder*. DefenseNews, 2012.

Obama, Barack. *Remarks by the President on Securing our Nation's Cyber Infrastructure*., 2009.

Oliker, Olga, Keith Crane, Lowell H. Schwartz, and Catherine Yusupov. *Russian Foreign Policy: Sources and Implications*. Santa Monica, CA: RAND Project Air Force, 2009.

Panetta, Leon E.. *America's Pacific Rebalance* In *Project Syndicate*., 2012.

PKI Cross-Certification Between CCEB Nations. Combined Communications-Electronics Board, 2007.

R. Nation, Craig. "*Results of the "Reset"*." In *US-Russian Relations*, 9. Vol. Russie.Nei.Visions No. 53 . Paris: IFRI, 2010.

Rauscher, Karl Frederick, and Valery Yashchenko. *Russia–U.S. Bilateral on Cyber Security: Critical Terminology Foundations*. New York and Moscow: EastWest Institute and Moscow State University, 2011.

Russia Calls for Cooperation in Combating Child Pornography. Voice Of Russia Radio, 2012.

Russia's National Security Strategy to 2020. National Security Council of the Russian Federation, 2009.

S., Nye Joseph. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* (2011): 31.

Sanger, David E.. "Obama Order Sped Up Wave of Cyberattacks Against Iran." *The New York Times* (2012).

Schmidt, Howard. *U.S. and Russia: Expanding the "Reset" to Cyberspace* In *The White House Blog*., 2011.

Schmitt, Michael N.. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013.

Securing Cyberspace for the 44th Presidency. Report of the CSIS Commission on Cybersecurity for the 44th Presidency. Washington, D.C.: Center for Strategic and International Studies, 2008.

Sestanovich, Stephen. *Reassessing the U.S.-Russia 'Reset'* In *Interview by Bernard Gwertzman*. Council on Foreign Relations Web Site, 2012.

Shackelford, Scott J.. "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law." *Berkeley Journal of International Law* 27 (2009): 196-97.

Sherr, James. *NATO and Russia: Doomed to Disappointment?*. NATO Review, 2011.

Shleifer, Andrei, and Daniel Treisman. "Why Moscow Says No." *Foreign Affairs* (2011): 122-38.

Shogren, Elizabeth. "U.S., Russia Cooperate on Y2K Concerns." *Los Angeles Times* (1999).

Soboleva, Inna. *NATO, Russia Consider Joint Missile-Defense System*. Russia Beyond the Headlines, 2013.

Spade, Jayson M.. *China's Cyber Power and America's National Security*. Carlisle, PA: U.S. Army War College, 2012.

Stavridis, James C., and Elton C. Parker. "Sailing the Cyber Sea." *Joint Forces Quarterly* 65 (2012): 62.

Stavridis, James G.. *Testimony before the 113th Congress, House and Senate Armed Services Committee Testimony*., 2013.

Sternstein, Aliya. *U.S., Russia, Other Nations Near Agreement on Cyber Early-Warning Pact*. Nextgov, 2012.

Strategy for Operating in Cyberspace. Washington, DC: United States Department of Defense, Government Printing Office, 2011.

The Applicability of International Law in Cyberspace-From If to How?. Panel Three at the Georgetown University Conference on the International Law on Cyber, 2013.

The G8 24/7 Network of Contact Points Protocol Statement., 2007.

The Right Direction for U.S. Policy toward Russia. Washington, D.C.: The Nixon Center, 2009.

Thomas, Timothy L.. *Recasting the Red Star: Russia Forges Tradition and Technology through Toughness* . Fort Leavenworth, KS: Foreign Military Studies Office, 2011.

Thomas, Timothy. "*Nation-State Cyber Strategies: Examples From China and Russia*." In *Cyberpower and National Security*, 475-76. Washington, D.C.: National Defense University Press, 2009.

Tikk, Eneken, Kadri Kaska, and Liis Vihul. *International Cyber Incidents: Legal Considerations*. Tallinn, Estonia: Cooperative Cyber Defence Center of Excellence, 2010.

Trenin, Dmitri. *The Russian Awakening*. Moscow: Carnegie Moscow Center, 2012.

Underground Economies: Intellectual Capital and Sensitive Corporate Data Now the Latest Cybercrime Currency. McAfee and SAIC, 2011.

Whitlock, Craig. "'Reset' Sought on Relations with Russia, Biden Says." *Washington Post* (2009).

Wilson, Clay. "*Cyber Crime*." In *Cyberpower and National Security*, 415. Washington, D.C.: National Defense University Press, 2009.