НОВЫЙ ПРИОРИТЕТ ДЛЯ РОССИЙСКОЙ ПУБЛИЧНОЙ ДИПЛОМАТИИ: ПРЕДОТВРАЩЕНИЕ КИБЕРАТАК НА ОБЪЕКТЫ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

О. В. Демидов

ПИР-Центр, Россия, 119019, Москва, 4-й Добрынинский пер., д. 8.

В статье рассматривается проблема кибернетических атак на объекты критической инфраструктуры, включая объекты атомной промышленности. На сегодняшний день международно-правовые нормы практически не охватывают использование информационно-коммуникационных технологий в целях нанесения ущерба информационным системам, обеспечивающим деятельность объектов критической инфраструктуры. В последние годы происходит беспрецедентный рост угроз объектам критической инфраструктуры, обусловленных бурным развитием информационно-коммуникационных технологий. Как стало известно в 2010 г., ряд государств Ближнего Востока, в первую очередь Иран, с 2008 г. подвергались серии систематических и беспрецедентно изощренных компьютерных атак неизвестного авторства, направленных прежде всего на сбор информации об объектах критической инфраструктуры данных стран, а также на программное поражение информационной инфраструктуры данных объектов. Автор поддерживает тезис о необходимости скорейшей выработки международно-правовых инструментов предотвращения и запрещения подобных кибератак. При этом бремя лидерства в постановке и решении данной задачи на международной арене может взять на себя Российская Федерация, чьи инициативы еще с 1998 г. задают глобальную повестку дня в части регулирования поведения государств в киберпространстве. Несмотря на существенные расхождения различных государств в данной сфере, их позиции в части обеспечения защиты от кибератак мирной атомной инфраструктуры наиболее близки к консенсусу, что создает коридор для практического продвижения в этом вопросе уже в 2013–2014 гг.

Ключевые слова: атомная отрасль, кибербезопасность, кибератаки, международная информационная безопасность, международное право, киберпространство.

На сегодняшний день международно-правовые нормы практически не охватывают использование информационно-коммуникационных технологий в целях нанесения ущерба информационным системам, обеспечивающим деятельность объектов критической инфраструктуры. Многие из таких объектов (предприятия топливно-энергетического комплекса, энергораспределяющие сети, системы контроля и управления наземным, морским и в особенности воздушным трафиком) в случае поражения программными средствами могут представлять угрозу национальной и международной безопасности.

Особое значение в этой связи имеют объекты мирной атомной отрасли и элементы инфраструктуры национальных программ развития атомной энергетики – атомные электростанции, обогатительные предприятия, инфраструктура хранения, транспортировки и утилизации отходов атомной промышленности. Недавняя авария на АЭС «Фукусима-1» в Японии в 2011 г. наглядно подтверждает тезис о том, что обеспечение безопасности объектов мирной атомной инфраструктуры и их защищенности от всевозможных факторов риска и угроз является задачей не только национального, но и международного уровня, решение которой должно значиться в числе приоритетов международного сообщества.

Между тем за последние годы происходит беспрецедентный рост угроз объектам критической инфраструктуры, обусловленных бурным развитием информационно-коммуникационных технологий. Как стало известно в 2010 г., ряд государств Ближнего Востока, в первую очередь Иран, с 2008 г. подвергались серии систематических и беспрецедентно изощренных компьютерных атак неизвестного авторства, направленных прежде всего на сбор информации об объектах критической инфраструктуры данных стран (в том числе объектах ТЭК и атомной отрасли), а также на программное поражение информационной инфраструктуры данных объектов. Характер деятельности, технические характеристики ряда программных средств, использованных для осуществления атак (в том числе компьютерных программ Gauss, Ma(h)di, Duqu, Flame, Wiper, Stuxnet и ряда других) привели международное экспертное сообщество к выводу о том, что для создания использовались ресурсы, доступные лишь государственным структурам, а цели применения данных программных средств лежат не в криминальной, а в международно-политической плоскости.

При этом эффект от поражения программными средствами объектов критической инфраструктуры уже не исчерпывается похищением данных, а переходит в плоскость нанесения физического ущерба работе промышленных и логистических объектов вплоть до их полного разрушения. Символом беспрецедентной опасности кибернетических атак стал компьютерный червь Stuxnet, который в 2009–2010 гг. поразил информационные системы иранского комбината по обогащению урана в г. Натанз, результатом чего стало разрушение более чем 100 центрифуг, предназначенных для обогащения урана, и нанесен стратегический ущерб развитию иранской атомной программы. Дальнейшее развитие подобных средств программного воздействия уже позволяет применять их для осуществления диверсий на электростанциях, в том числе для разрушения энергогенерирующих турбин атомных электростанций и тому подобных составляющих критической атомной инфраструктуры. Подобные последствия выходят за рамки национальных границ государств, чья инфраструктура подвергается атакам, и представляют непосредственную угрозу международной безопасности наравне с международным терроризмом, трансграничной преступностью, а в перспективе и использованием оружия массового уничтожения.

Разработка и применение подобных программных инструментов осуществляется анонимно, в силу того что существующие технические возможности не позволяют достоверно и однозначно идентифицировать конечный источник атаки и непосредственного ее автора. Кроме того, даже при наличии технической возможности определить, откуда осуществляется атака, не существует каких бы то ни было юридических и международно-правовых механизмов, позволяющих отнести ответственность за осуществление такой деятельности с конкретным лицом и тем более субъектом международного права.

Таким образом, международное сообщество сегодня находится в ситуации, когда действующие нормы международного права ни в коей мере не регулируют использование в деструктивных целях информационных технологий, потенциал которых приближается к оружию массового уничтожения. Отсутствие единого международно-правового режима противодействия кибернетическим угрозам в отношении объектов критической, и в том числе атомной инфраструктуры, обуславливает непосредственную опасность расшатывания фундамента международной безопасности и стабильности, а также создает риск дальнейшего роста подобного рода атак.

Российская Федерация, как государство, занимающее лидирующие позиции в мире в области атомной энергетики и обладающее сложной и высокоразвитой инфраструктурой атомной энергетики, как и немногие другие участники международного сообщества, заинтересована в обеспечении безопасности объектов мирной атомной отрасли, в том числе от угроз,. Именно РФ впервые поставила на глобальную повестку дня вопрос о формировании международно-правового режима обеспечения международной информационной безопасности (МИБ). С 1998 г. по российской инициативе был принят ряд резолюций Генеральной ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», в которых, в частности, отмечается целесообразность строительства международно-правовых режимов с целью запрещения разработки особо опасных форм информационного оружия [1].

В настоящее время Российская Федерация продолжает акцентировать внимание на выработке международно-правового инструментария по запрету политически мотивированной агрессии в информационном пространстве, занимая в этой сфере лидерские позиции. Сегодняшнее российское видение проблематики обеспечения международной информационной безопасности с учетом национальных интересов и потребностей международного сообщества во многом суммирует концепция Конвенции об обеспечении МИБ, обнародованная в ноябре 2011 г., а также Правила поведения в области обеспечения МИБ, направленные Генеральному секретарю ООН в сентябре 2011 г. письмом за подписью представителей РФ, КНР Таджикистана и Узбекистана. Ключевыми приоритетами в рамках этих инициатив являются предотвращение военных конфликтов в информационном пространстве, и сотрудничество государств в определении источников кибератак [2].

Принятие предложенного Россией проекта документа в качестве Конвенции ООН могло бы стать шагом вперед в задаче обеспечения безопасности критической инфраструктуры от кибератак. Однако на данный момент российский подход по ряду причин наталкивается на серьезные противоречия, связанные с неприятием комплексного и всеобъемлющего характера российских инициатив рядом других государств. Дискуссии в ходе Международных конференций по киберпространству в Лондоне (2011 г.) и Будапеште (2012 г.) показали, что западные партнеры России не готовы поддерживать российскую концепцию Конвенции, равно как и ставить подпись под иными международными соглашениями, фиксирующими широкий круг их обязательств в части поведения в информационном пространстве.

В этих условиях на первый план выходит выработка точечного, предметного международно-правового механизма, проблематика которого будет ограничена вопросами защиты объектов атомной отрасли от кибератак как от наиболее острой и чреватой катастрофическими последствиями угрозы МИБ. Такой механизм, в частности, может включать в себя адаптацию действующих норм международного гуманитарного права (Гаагских, Женевских конвенций и Дополнительных протоколов к последним) в части ненападения на невоенные объекты и объекты гражданской инфраструктуры [3].

Однако такая задача в настоящее время не акцентирована и не сформулирована четко как российским МИД, так и зарубежными партнерами России. Одной из причин такой ситуации является то, что вопросы использования международно-правового инструментария для предотвращения и запрещения кибератак на мирные атомные объекты недостаточно активно поднимаются российскими и международными экспертами. В частности, уровень вовлеченности российских экспертов в международную дискуссию по этому вопросу сегодня недопустимо низок – прежде всего в смысле практически полного отсутствия международных площадок, где российские и зарубежные специалисты имели бы возможность совместно и подробно проработать эту проблему. Кроме того, для нахождения эффективных решений в этой области необходимо обеспечить совместную работу междисциплинарной (и международной группы) технических специалистов, экспертов по международному праву, а также дипломатов и международных чиновников.

При этом угроза катастрофических атак в политических целях на объекты атомной отрасли и иные объекты атомной инфраструктуры нарастает с каждым годом – с момента обнаружения Stuxnet уже выявлено порядка 10 схожих программ, которые превосходят своего предшественника по сложности исполнения и разнообразию возможностей. 2013 и 2014 гг. должны стать поворотной точкой в активизации усилий международного сообщества в направлении решения этой проблемы на уровне международного права. Российская Федерация, традиционно выступающая лидером в сфере международных инициатив по обеспечению МИБ, имеет все шансы сыграть ключевую роль в этом вопросе. Однако для этого необходимо активизировать усилия российской публичной дипломатии, которая пока не еще не проявила себя в этом направлении, а также в короткие сроки, не позднее начала 2014 г., обеспечить ее мощным импульсом экспертной поддержки, отражающим приоритет российских национальных интересов в сфере международно-правового предотвращения и запрещения кибернетических атак на атомную инфраструктуру и иные критически важные объекты.

Список литературы

1. Developments in the Field of Information and Telecommunications in the Context of International Security. Fact Sheet. NewYork. United Nations Office for Disarmamnet Affairs, 2013
2. Mauer, T. (2011, September). Explorations in Cyber International Relations Discussion Paper Series. Discussion Paper #2011-11. Belfer Center for Science and International Affairs. Harvard Kennedy School: Available at: http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf
3. Rausher, K., & Korotkov, A. (2011). Working Towards Rules for Governing Cyber Conflict. Rendering the Geneva and Hague Conventions in Cyberspace . East West Institute. Available at: http://www.ewi.info/working-towards-rules-governing-cyber-conflict.

Об авторе

Демидов Олег Викторович – координатор программы «Международная информационная безопасность и глобальное управление Интернетом» ПИР-Центра, аспирант МГИМО(У) МИД России. E-mail: vestnik@mgimo.ru

PREVENTING CYBER ATTACKS ON CRIRICAL INFRASTRUCTURE: A NEW PRIORITY FOR THE RUSSIAN PUBLIC DIPLOMACY?

O.V. Demidov

PIR Center, Moscow, 119019, 4th Dobryninsky pereulok, 8.

Abstract: *The article analyses the problem of cyber attacks on critical infrastructure, including facilities of the nuclear industry. At present there is almost no international legal regulation of the possible usage of information technologies in order to information systems used by object of the critically important infrastructure. Still, there has been an unprecedented growth in the information threats in recent years. As it was revealed in 2010, several Middle East States, first of all Iran in 2008, were the target for a series of systematic and sophisticated computer attacks, whose initiators remain unknown, which were aimed at the collection of information about the objects of critical information infrastructure of these states and its program intrusion. The author supports the thesis of the need for early development of international legal instruments to prevent and prohibit such cyber attacks. At the same time the leadership in the formulation and solution of this problem on the international scene can assume the Russian Federation, whose initiatives have since 1998 shaped the global agenda in terms of regulating the behavior of states in cyberspace. Despite the significant differences of different countries in this area, their positions on ensuring protection against cyber attacks peaceful nuclear infrastructure are the closest to a consensus, creating a window of opportunity for practical progress on this issue in 2013-2014.*

Keywords: critical infrastructure, cybersecurity, cyberspace, cyber attacks, international law, nuclear industry, Stuxnet.

References

1. Developments in the Field of Information and Telecommunications in the Context of International Security. Fact Sheet. NewYork. United Nations Office for Disarmamnet Affairs, 2013
2. Mauer, T. (2011, September). Explorations in Cyber International Relations Discussion Paper Series. Discussion Paper #2011-11. Belfer Center for Science and International Affairs. Harvard Kennedy School: Available at: http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf
3. Rausher, K., & Korotkov, A. (2011). Working Towards Rules for Governing Cyber Conflict. Rendering the Geneva and Hague Conventions in Cyberspace . East West Institute. Available at: http://www.ewi.info/working-towards-rules-governing-cyber-conflict.

About the author

Demidov O. Viktorovich – coordinator of the program "International Information Security and Global Internet Governance" at the Center of Political Research of Russia (PIR- Center). E-mail: vestnik@mgimo.ru