№ 56 ВАЛДАЙСКИЕ ЗАПИСКИ

Сентябрь, 2016

Валдай | Международный дискуссионный клуб
www.valdaiclub.com

ЯДЕРНОЕ ОРУЖИЕ В ВЕК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ: НОВЫЕ ВЫЗОВЫ С ТОЧКИ ЗРЕНИЯ БЕЗОПАСНОСТИ, СТРАТЕГИИ И СТАБИЛЬНОСТИ

Эндрю Футтер

Об авторе:

Эндрю Футтер

Старший преподаватель Факультета политологии и международных отношений Университета Лестера; научный сотрудник Академии высшего образования Великобритании

Данный текст отражает личное мнение автора,
которое может не совпадать с позицией Клуба, если явно не указано иное.

Обеспечение безопасности и надежности в управлении системами и арсеналами ядерного оружия всегда было непростым делом, сопряженным с рисками и неопределенностью. С появлением новых кибертехнологий и связанных с ними потенциальных угроз, в том числе со стороны хакеров, стремящихся получить доступ к системам ядерного оружия или взломать их, эта задача стала еще более сложной. Спектр вызовов широк: от безопасности, защиты и надежности систем командования и управления ядерным оружием – до появления новых проблем в области информбезопасности, распространения ядерного оружия и обеспечения режима строгой секретности в отношении стратегических ядерных технологий, проблем стратегического сдерживания и эскалации, а также обеспечения кибербезопасности ядерных объектов.

Ядерное оружие все еще остается наиболее важным атрибутом национальной безопасности – киберугрозы пока не претендуют на такую роль. Но сохранность и безопасность таких систем все чаще оказывается под вопросом, в связи с чем для ядерных держав все более актуальной становится проблема стратегии управления ядерными силами. Обеспечение кибербезопасности требует гибкого и тонкого подхода, поскольку появление киберугроз привело не столько к радикальному изменению систем командования и управления ядерным оружием, сколько к еще большему усложнению проблем, которые и без того были присущи этим системам. Эти новые вызовы свидетельствуют об изменении дискурса о ядерном оружии, управлении государствами своими ядерными силами, ядерной политике и стратегии. Соответственно, эта проблема прямо или косвенно затрагивает не только вопросы ядерной безопасности и функционирования систем командования и управления ядерным потенциалом, но и тему поддержания стратегического баланса сил, сохранения в силе соглашений по контролю над вооружениями и сокращения ядерных арсеналов в будущем.

Природа проблем, связанных с киберпространством

Природа и значение понятия «кибер»[1] являются предметом разногласий в экспертном сообществе и по-разному трактуются различными государствами, организациями и экспертами. Не существует единого, общепризнанного определения. В итоге, на основе разных посылов делаются разные выводы и предлагаются разные решения связанных с киберпространством проблем. Все это значительно усложняет изучение и обсуждение этой проблематики. В то время как некоторые авторы придерживаются узкой трактовки концепции кибербезопасности, уделяя основное внимание сетевым операциям (Computer Network Operations, CNO) и интернет-атакам, существует более широкая интерпретация, согласно которой кибербезопасность относится к сфере информационных войн и является их составной частью. Некоторые эксперты идут еще дальше, рас-

[1] *Cyber – виртуальный, относящийся к киберпространству.*

сматривая концепцию кибербезопасности как комплексное понятие, влияющее на все аспекты национальной безопасности. Существуют разные подходы и в том, что касается классификации кибератак и значения этого термина. К кибератакам относят как обычные хакерские атаки, в том числе во имя политических и религиозных целей (так называемый «хактевизм»), киберпреступность, DoS-атаки и кибершпионаж, так и подрывную деятельность, разрушение объектов инфраструктуры и даже военные действия. Многие проблемы, с которыми сталкиваются эксперты в области кибербезопасности, обусловлены разнообразием и масштабом киберугроз, что, в свою очередь, является основной причиной разногласий по вопросу об их уровне и природе.

При рассмотрении проблем, с которыми сталкивается атомная промышленность, необходимо принимать во внимание все аспекты, связанные с киберпространством, и руководствоваться наиболее широким определением этого понятия с учетом физических, информационных и когнитивных аспектов, а также логики сетевых операций. Такой подход позволит поставить в данной работе вопрос о влиянии киберпространства в наиболее широком понимании этого термина на концепции и стратегии, касающиеся ядерного оружия. При таком подходе понятие «cyber» относится к операционной среде, наступательному потенциалу, уровню общественного развития, а также к различным силам. Хакерские атаки представляют большую угрозу, но это не единственный феномен, способный воздействовать на институты, специализирующиеся на ядерном оружии. В этой связи представляется целесообразным использовать термин «вызов кибербезопасности», под которым следует понимать все потенциальные направления атак: нанесение ущерба, уничтожение, срыв или установление контроля над различными видами деятельности, связанными с компьютерами, сетями, программным и аппаратным обеспечением или инфраструктурой, а также связанными с ними людьми[2].

Кибератаки против систем ядерных вооружений могут иметь *физический* характер, например, когда объектом нападения являются компьютеры, аппаратное обеспечения, узлы связи, проводка и кабели, оборудование, обеспечивающее распространение и хранение информации. Такие атаки также могут происходить на *программном* уровне, например, когда их объектом становятся операторы аппаратного обеспечения и программное обеспечение, отвечающее за передачу, интерпретацию и обмен ключевой информацией. Кибертаки могут происходить в компьютерных сетях, по интернету или в отношении программного обеспечения, в частности, посредством заражения его компьютерными червями, логическими бомбами, вирусами-троянами; в результате обычных хакерских атак, а также атаки с целью завладения или порчи информации, на основе которой функционируют такие системы, или которую используют операторы[3]. Кроме того, понятие «вызов кибербезопасности» включает проблемы, являющиеся результатом естественного процесса все большего усложнения систем и обусловленные неуверенностью в надежности ключевых систем. Таким образом, понятие «вызов кибербезопасности» охватывает присущие системам ядерного оружия виды уязвимости, а также

---

[2] *Определение основано на работе Jason Andres & Steve Winterfield, "Cyber warfare: techniques, tactics and tools for security practitioners", (Waltham MA, Syngress: 2011), c.167.*

[3] *Согласно Lucas Kello "The meaning of the cyber revolution: perils to theory and statecraft", International Security, 38:2 (2013), c. 18.*

угрозу от лиц, стремящихся получить доступ к таким системам в целях внесения в них изменений, отключения, подрыва или нанесения им ущерба. Наконец, ключевым аспектом понятия «вызов кибербезопасности» является человеческий фактор, ведь именно люди проектируют системы и создают программное обеспечение, рассчитывая, что компьютеры и другое оборудования будут работать в штатном режиме.

Таким образом, этот вызов представляется многогранным и затрагивает все уровни: от безопасности отдельных объектов систем командования и управления ядерным оружием – до структур государственного значения, национальной стратегии в области безопасности, международных отношений по вопросу о стратегических видах вооружений и обеспечения стабильности на фоне кризисных явлений. Хотя такие вызовы нередко лишены каких-либо зримых проявлений, они, как правило, взаимосвязаны. Например, атака против системы предварительного оповещения о ядерном ударе может подорвать стабильность и лишить страну сдерживающего потенциала.

Таким образом, представляется целесообразным рассмотреть все три уровня функционирования ядерной отрасли: система ядерного вооружения внутри страны, государственная стратегия по ядерному оружию и международная система.

Новые виды уязвимости систем ядерного оружия

Системы ядерного оружия всегда находились под угрозой вмешательства и нападения извне. История знает множество примеров просчетов, аварий и ошибок, причем во многих случаях причиной становились компьютеры или компьютерные системы. Это обусловлено необходимостью обеспечения *подтверждающего контроля* (гарантия срабатывания в любых условиях) и *негативного контроля* (предупреждение случайного или несанкционированного использования). Таким образом, ядерное оружие всегда будет уязвимым перед лицом попыток вмешаться в работу систем подтверждающего или негативного контроля. Соответственно, киберугрозы не меняют, а скорее дополняют и делают еще более сложной систему командования и управления системами ядерного оружия (и связанной с ними инфраструктуры). В этом отношении необходимо обратить внимание на два аспекта. Во-первых, усложнение системы, в особенности ее компьютеризация и переход на цифровые технологии, повышает риск возникновения обычных аварий в отрасли. Кроме того, чем сложнее система управления ядерным оружием, тем больше в ней уязвимости, слабых сторон и ошибок, которые могут быть использованы хакерами.

Доказательством наличия в системах командования и управления ядерным оружием изначально заложенных в них видов уязвимости служат многочисленные аварии, промахи и просчеты прошлого. Согласно теории обычных аварий, сложные системы не всег-

да срабатывают и время от времени дают сбои. Особенно это относится к системам, подвергающимся высокому давлению из-за невозможности проведения исчерпывающих замеров, или к системам, связанным с опасными технологиями[4]. Системы командования и управления ядерным оружием – хороший пример сложной системы. В атомный век произошло немало аварий и допущено немало промахов. Многие, хоть и не все, были связаны с компьютерами и программным обеспечением. В будущем число таких аварий может вырасти по мере все большего усложнения систем управления ядерным оружием и их перевода на цифровые технологии.

Рост зависимости функционирования систем ядерного оружия от компьютеров и программного обеспечения, от систем раннего предупреждения, защиты, обработки и анализа данных – вплоть до санкционирования пуска и его осуществления, открывает перед хакерами новые возможности по использованию уязвимости таких систем. Одна из главных проблем заключается в том, что в системах командования и управления ядерным оружием используется все более совершенное и сложное программное обеспечение. В таком случае вероятность наличия в программном коде ошибок, проблем и непредвиденных недочетов выше, чем в обычном программном обеспечении, особенно если программный код сложен, сводит воедино множество функций и элементов аппаратного обеспечения и отвечает за выполнение точных вычислений в сжатые сроки. Именно такими слабыми местами в первую очередь пользуются хакеры для взлома систем и обхода их средств защиты. Это, очевидно, представляет угрозу для систем командования и управления ядерным оружием, а также может иметь серьезные последствия для работы всей ядерной отрасли в целом, в особенности в том, что касается безопасности секретной информации о ядерных технологиях.

Конечно, системы ядерного оружия всегда хорошо защищены от киберугроз и, как правило, не подключены к интернету. Однако их ни в коем случае нельзя считать неуязвимыми. Перед хакерами открывается реальная возможность спровоцировать пуск ядерного оружия или вывести из строя систему; подать ложный сигнал на датчики предупреждения, создать помехи связи, чтобы предотвратить поступление распоряжений, или получить доступ и использовать информацию об операционных процедурах высокой степени секретности. И вероятность такого сценарии только увеличивается. Это связано с ростом количества уязвимостей в программном обеспечении как в системах командования и управления ядерным оружием, так и на различных объектах инфраструктуры, задействованных в управлении такими системами.

Проблема заключается в том, что атака хакеров может быть направлена как на *выведение* системы из строя, так и для *провоцирования* пуска или взрыва. Наличие в программном обеспечении уязвимостей также позволяет с большей легкостью взламывать соответствующие системы, новыми способами красть данные, дестабилизировать различные системы посредством ошибочной информации, а также вмешиваться в деятельность, мешать или наносить ущерб объектам и процессам, имеющим важное значение.

---

[4] *Charles Perrow, "Normal accidents: living with high-risk technologies", (Princeton NJ, Princeton University Press: 1999).*

Ядерный кибершпионаж

Возможность кражи противником секретной информации о ядерном оружии (проекты систем, характеристики, оперативные планы и процедуры) всегда была актуальной для ядерных держав. Однако распространение компьютеров, сетевых технологий и цифровых форматов хранения данных привело к появлению новых проблем, связанных с обеспечением секретности, а также изменением и расширением арсенала и методов ядерного шпионажа. Проблема не только в возможности взлома секретных систем и скачивания информации в интернете, но и в степени защиты компьютеров и информации в рамках систем, которые не подключены к интернету. Обе проблемы стоят очень остро в силу хранения на компьютерах больших объемов информации, которая может быть украдена, причем (относительно) минимальными усилиями. При возможности проведения таких атак удаленно, нарушители подвергаются еще меньшему риску, поскольку не нужно кого-то отправлять на опасную операцию. Такие атаки достаточно эффективны в силу своей масштабности: ведь они направлены на то, чтобы украсть как можно больше информации о чем угодно, но при этом могут быть также нацелены на получение конкретной, специализированной информации.

Эпоха ядерного кибершпионажа началась в середине 1980-х годов, когда в организациях оборонного комплекса, в особенности в США, стали появляться компьютеры и внедряться сетевые технологии.

Одним из первых проявлений этого вида преступности стал эпизод, получивший название «Кукушкино яйцо» (1986 г.)[5]. В 1991 году голландские хакеры взломали сеть армии США в поиске ядерных секретов и данных о параметрах ракет, чтобы продать их Саддаму Хусейну[6]. В 1998 году из доклада члена Палаты представителей США Криса Кокса стало известно, что Китай украл большой объем информации высокой степени секретности о разработке термоядерной боеголовки W88[7]. В том же году хакер взломал компьютерную систему Атомного научно-исследовательского центра имени Хоми Бхабха в Индии, скачав пароли и данные электронной почты[8]. В 1999 году стало известно о масштабной атаке "*Moonlight Maze*" против Пентагона и объеме секретной информации, похищенной у органов государственной власти США[9].

За последнее десятилетие эта тенденция не только сохранилась, но и приобрела еще более выраженный характер. В 2005 году, в ходе операции, получившей название «Титановый дождь», хакеры, связанные с Народно-освободительной армией Китая, взломали ряд компьютерных сетей армии США[10]. В 2006 году Моссад заразил

---

[5] См. Clifford Stoll, "The cuckoo's egg: tracking a spy through the maze of computer espionage", (London, Doubleday: 1989).

[6] Dorothy Denning, "Information warfare and security", (Reading MA, Addison-Wesley: 1999).

[7] Из Vernon Loeb & Walter Pincus, "Los Alamos security breach confirmed", The Washington Post, (29 апреля 1999 г.), http://www.washingtonpost.com/wp-srv/national/daily/april99/spying29.htm.

[8] Adam Penenberg, "Hacking Bhabha", Forbes, (16 ноября 1998 г.), http://www.forbes.com/1998/11/16/feat.html.

[9] Adam Elkus, "Moonlight Maze", глава из Jason Healey (Ed), "A fierce domain: conflict in cyberspace, 1986–2012", (USA, Cyber Conflict Studies Association: 2013), с. 155.

[10] William Hagestad, "21st century Chinese cyberwarfare", (Ely, IT Governance Publishing: 2010), с. 12.

вирусом компьютер одного сирийского чиновника – израильская разведка, таким образом, получила информацию о масштабах программы по созданию ядерного оружия, которая предположительно велась в Сирии. Что и стало основанием для проведения операции «Фруктовый сад» в 2007 году (см. далее)[11]. В 2008 году, из-за оставленного на парковке USB-накопителя США подверглись нападению в ходе операции «Buckshot Yankee». Были взломаны секретные сети и получен доступ к компьютерам, не имевшим связи с интернетом[12]. В 2011 году обнаружен вирус-троян «Зевс», который использовался против подрядчиков, участвовавших в создании Великобританией подводных лодок, оснащенных БРПЛ Trident[13]. В том же году Иран обвинили в проведении хакерской атаки против МАГАТЭ[14]. Был обнаружен компьютерных червь "Shady RAT", который использовался против государственных ведомств США, оборонных подрядчиков и высокотехнологических компаний[15]. В 2012 году группа хакеров «Анонимус» пригрозила раскрыть украденную у МАГАТЭ секретную информацию по ядерной программе Израиля[16].

На протяжении последнего десятилетия главной мишенью были лаборатории и оборонные подрядчики США[17]. Кроме того, объектами хакерских атак также становились программы противоракетной обороны США и Израиля[18]. Хотя значительная часть попыток кражи информации о ядерном оружии была направлена против США, операция «Олимпийские игры», одним из результатов которой стало появление компьютерного вируса Stuxnet, изначально была нацелена на сбор информации о ядерных объектах Ирана. Аналогичным образом компьютерные черви "Flame" и "Duqu" были созданы для получения разведданных о системах и инфраструктуре, став, по всей видимости, провозвестниками действий по срыву иранской ядерной программы[19].

---

[11] Eric Follarth & Holger Stark, "The story of Operation Orchard: how Israel destroyed Syria's Al Kibar nuclear reactor", Spiegel Online, (2 ноября 2009 г.), http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html.

[12] Karl Grindal, "Operation Buckshot Yankee", глава из Jason Healey (eds.), "A fierce domain: conflict in cyberspace 1986 to 2012", (USA, Cyber Conflict Studies Association: 2013), с. 208.

[13] Richard Norton-Taylor, "Chinese cyber-spies penetrate Foreign Office computers", The Guardian, (4 февраля 2011 г.), http://www.theguardian.com/world/2011/feb/04/chinese-super-spies-foreign-office-computers.

[14] David Crawford, "UN probes Iran hacking of inspectors", Wall Street Journal, (19 мая 2011 г.), http://www.wsj.com/articles/SB10001424052748704281504576331450055868830.

[15] William Hagestad, "21st century Chinese cyberwarfare", (Ely, IT Governance Publishing: 2010) с. 12.

[16] Michael Kelley, "Anonymous hacks top nuclear watchdog again to force investigation of Israel", Business Insider, (3 декабря 2012 г.), http://www.businessinsider.com/anonymous-hack-iaea-nuclear-weapons-israel-2012-12?IR=T.

[17] "US nuclear weapons researchers targeted with Internet Explorer virus", Russia Today, (7 мая 2013 г.), http://rt.com/usa/attack-department-nuclear-internet-955/.

[18] См. Andrew Futter, "Hacking missile defense: the cyber challenge to BMD", The Missile Defense Review, (1 марта 2015 г.), http://missiledefensereview.org/2015/03/01/hacking-missile-defence-the-cyber-challenge-to-bmd/.

[19] Chris Morton, "Stuxnet, Flame and Duqu – the Olympic Games", глава из Jason Healey (eds.), "A fierce domain: conflict in cyberspace 1986 to 2012", (USA, Cyber Conflict Studies Association: 2013) с. 219–221.

Все эти действия имели противоречивые последствия. Наиболее простым видом кибершпионажа в целях получения информации о ядерном оружии является деятельность по получению информации о действиях определенного государства или организации и потенциале ядерной программы. На следующем уровне, секреты могут быть использованы для борьбы с определенными системами или защиты от них, а также для получения операционных данных. Еще большую озабоченность вызывает кража секретной информации о ядерном оружии в целях его распространения, а также для торговли проектами и чертежами на черном рынке ядерных технологий. Наконец, атаки могут быть провозвестником подрывных операций и быть нацеленными на получение информации о расположении ядерных объектов и их уязвимости, размещения логических бомб и обеспечения доступа к системам в дальнейшем.

Создание помех, искажение информации, диверсии

С компьютеризацией общества значительно возросли возможности осуществления диверсий на важнейших системах обеспечения безопасности, включая национальную инфраструктуру и системы ядерных вооружений. Существует опасность отдельных ограниченных атак, как направленных против ядерных сил и систем ядерных вооружений, так и не направленных против ядерного оружия непосредственно, но способных оказать на него отрицательное воздействие. Хотя ядерные системы наверняка защищены от диверсий и атак намного лучше, чем гражданская инфраструктура, упомянутая опасность существует реально, и ее признаки заметны во всех отраслях, имеющих отношение к производству ядерного оружия.

Со значительным риском сопряжена, например, поставка заказчикам ядерного ПО и компонентов ЯО. Дело в том, что внедрение логических бомб, троянов для ПО и ЭВМ может произойти сразу на нескольких этапах: этапе производства, поставки и обслуживания. Диверсионная деятельность может принимать разные обличья: физическое изменение компонентов с тем, чтобы в определенный момент они либо переставали функционировать вовсе, либо функционировали не так, как положено; внедрение вредоносных программных средств или преднамеренно модифицированных кодов для видоизменения процессов, либо установка вредоносных программ, позволяющих в дальнейшем осуществлять доступ к системам с тем, чтобы управлять протекающими в них процессами, препятствовать им, или их останавливать.

Кибердиверсионная деятельность зародилась в 80-х годах прошлого века, когда ЦРУ США организовало поставку в СССР модифицированного технического и компьютерного оборудования. В рамках операции под кодовым названием

«Прощальное досье» советскому военно-промышленному комплексу были подброшены дефектные компьютерные микросхемы и фальшивые чертежи[20]. В 90-е годы прошлого века США и Израиль внесли изменения в конструкцию вакуумных насосов, закупавшихся Ираном, с тем, чтобы обеспечить их дальнейший выход из строя[21]. В 2012 году фирму «Сименс» обвинили в установке взрывных микроустройств в оборудование, закупленное Ираном для своей ядерной программы[22]. А в 2014 году Иран обвинил Запад в том, что тот «пытается вывести из строя расположенный в Араке ядерный реактор на тяжелой воде путем замены компонентов его системы охлаждения»[23].

Кибердиверсионная деятельность также включает в себя попытки атаковать, вскрывать или обманывать системы раннего оповещения и системы связи, а также выхолащивать информацию, которой руководствуются принимающие решения инстанции и системы. Важнейшими составляющими боевых действий издавна были попытки заблокировать каналы связи противника и перехитрить его, подсунув ложную информацию, но в век кибернетики эта тактика также меняется. Лучший тому пример – использование Израилем в 2007 году для блокирования сирийского радара ПВО военной программы «Сутер», что позволило разбомбить предполагаемый ядерный объект. Вместо того, чтобы просто глушить сигналы радара, «Сутер» [якобы] внедрился в систему ПВО Сирии и тем самым позволил израильским самолетам беспрепятственно отбомбиться по намеченной цели[24]. Хотя и ограниченная по своему масштабу, эта атака послужила жестким предупреждением о наличии новых уязвимых мест в системах безопасности, особенно в системах ядерных коммуникаций и раннего предупреждения.

Наконец, некоторые атаки направлены на то, чтобы вызвать физические разрушения или ядерный взрыв. Хотя испытание в 2007 году генератора Aurora и выявило возможности для осуществления диверсий с помощью киберсредств, лишь немногие кибератаки вызвали физические разрушения, о которых известно широкой публике. И только одна из них (с использованием компьютерного червя Stuxnet) нанесла непосредственный урон ядерному объекту (хотя ходят слухи об американских атаках на объекты ядерной программы КНДР[25]). Stuxnet, по-видимому, проник в отключенную от Интернета сеть комбината в Нетензе с инфицированного USB-накопителя или иного устройства по не-

---

[20] Gus Weiss, "Duping the Soviets: the Farewell Dossier", Studies in Intelligence, 39:5 (1996), с. 125.

[21] David Sanger, "Confront and conceal: Obama's secret wars and surprising use of American power", (New York, Broadway Paperbacks: 2013), с. 194.

[22] "Iran says nuclear equipment was sabotaged", New York Times, (22 сентября 2012 г.), http://www.nytimes.com/2012/09/23/world/middleeast/iran-says-siemens-tried-to-sabotage-its-nuclear-program.html?_r=0.

[23] David Sanger, "Explosion at key military base in Iran raises questions about sabotage", New York Times, (9 октября 2014 г.), http:// www.nytimes.com/2014/10/10/world/explosion-at-key-military-base-in-iran-raises-questions-about-sabotage.html.

[24] Richard Clarke & Robert Knake, "Cyber war: the next threat to national security and what to do about it", (New York, HarperCollins: 2010), с. 6–8.

[25] Salvador Rodriguez, "US tried, failed to sabotage North Korea nuclear weapons program with Stuxnet-style cyber-attack", International Business Times, (29 мая 2015 г.), http://www.ibtimes.com/us-tried-failed-sabotage-north-korea-nuclear-weapons-program-stuxnet-style-cyber-1945012.

досмотру беспечного служащего, имевшего доступ к источникам инфекции. Но предварительно сеть изучили и создали ее карту[26].

И Stuxnet, и операция «Фруктовый сад» – суть свидетельства того, что при самом неблагоприятном развитии событий возможно выведение из строя даже тех сетей, которые считаются не подсоединенными к Интернету, а также систем, жизненно необходимых для функционирования ядерных объектов. Основной проблемой остается риск непрямого вмешательства, а также вмешательства третьих сторон. Небезынтересно в этой связи то, что более старые и менее изощренные системы и объекты инфраструктуры, используемые в управлении системами ядерных вооружений, более безопасны и лучше защищены от (кибер-) диверсий и помех.

Стратегическая стабильность и антикризисное управление

В прошедшем десятилетии все более значимыми элементами противостояния были хакеры и кибератаки. Хотя кое-кому и может показаться, что киберпространство существует отдельно от остального мира, но в действительности разделить их не представляется возможным. Именно поэтому киберпространство и будет играть в дальнейшем важную роль в процессе принятия решений по ядерному оружию и в поддержании стратегического равновесия. Эксплуатация киберпространства и кибератаки (осуществленные либо в автономном режиме, либо во взаимодействии с подвижными военными силами) приобретают все большее значение, и это может повлиять на характер вооруженной борьбы, стратегическую стабильность и в особенности – на практику антикризисного управления в исполнении обладателей ядерного оружия.

Кибератаки могут воздействовать на стратегическую и кризисную стабильность в среде обладающих ядерным оружием акторов в четырех главных областях[27].

Во-первых, хакеры гипотетически способны нарушить работу каналов связи или полностью вывести их из строя, тем самым осложнив управление ядерными силами и подорвав доверие командиров к собственным системам. Для нарушения связи, создания помех в системах управления боем и затруднения процесса оценки обстановки могут быть запущены распределенные атаки типа «отказ в обслуживании» (DDoS).

Во-вторых, они способны создать обостренное ощущение спешки у тех, кто занят выработкой решения на удар/ответный удар или превентивный удар.

---

[26] *Jon Lindsay, "Stuxnet and the limits of cyber warfare", Security Studies, 22:3 (2013), с. 381.*

[27] *Излагается по: Stephen Cimbala, Nuclear Weapons in the Information Age, London, Continuum International Publishing, 2012, с. 56–57.*

В-третьих, они могут спровоцировать свертывание поиска реальных альтернатив, тем самым сокращая время развития процесса.

В-четвёртых, они способны повысить неопределенность ситуации, создать неверное представление о намерениях сторон и о наличии у них сил и средств, либо спровоцировать нештатное срабатывание систем раннего оповещения (что чревато особой опасностью, учитывая возможность провокационных вылазок третьих сторон), усугубить опасения по поводу вероятности внезапного удара стратегическими средствами, и создать помехи в системе сигнализации. В совокупности такие воздействия повышают вероятность случайной эскалации, превращая управление кризисной ситуации в еще более трудное и опасное дело.

Скорее всего, основное соперничество на этом направлении развернется между США и Китаем, так как в обоих государствах не скрывают, что им известно значение кибер-средств борьбы и атак на информационные системы. Главным образом здесь следует опасаться стремительного перерастания незначительного конфликта в стратегический. Но существует (особенно в Китае) и опасность кибератак на систему управления ядерными силами и смежные объекты и их повреждения с помощью электронных средств нападения. В таком случае Китаю будет непросто соблюдать обязательство о неприменении ядерного оружия первым, особенно ввиду наличия у США системы противоракетной обороны и ударных неядерных сил.

Соперничество иного порядка возможно между США и их союзниками по НАТО, с одной стороны, и Россией – с другой. В НАТО открыто заявляют, что главным вызовом и предметом озабоченности для альянса являются кибератаки, и что некоторые из них «могут нанести странам НАТО и их экономикам такой же тяжелый урон, как и война с применением обычных видов оружия»[28]. Как в НАТО, так и в России признают ядерное сдерживание: на боевом дежурстве там остается значительное число ядерных средств.

Хотя угроза эскалации под воздействием провокаций в киберпространстве является важным аспектом стратегического баланса в отношениях между Востоком и Западом, особенно актуальной остается прямая и косвенная киберугроза ядерным силам США и России. В число таких вызовов входят атаки, направленные на нейтрализацию систем управления ядерными вооружениями, их повреждение или разрушение. Кроме того, возможны атаки третьих сторон, стремящихся ускорить наступление кризиса, усугубить его, и даже спровоцировать ядерный пуск. Хотя эти вызовы идентичны тем, что стоят перед парой США–Китай, в отношениях между США и РФ они усугубляются наличием огромных запасов ядерных вооружений, в частности МБР, которые обеими сторонами поставлены на боевое дежурство. В ходе любого возможного в будущем кризиса эти вызовы будут только умножаться.

---

[28] Warwick Ashford, "Nato to adopt new cyber defence policy", ComputerWeekly.com, (3 сентября 2014 г.), http://www.computerweekly.com/news/2240228071/Nato-to-adopt-new-cyber-defence-policy.

Сдерживание кибератак с помощью ядерного оружия?

Угроза крупномасштабной кибератаки выдвигает целый ряд новых требований к национальной политике в области безопасности и роли ядерного оружия. Выработка действенного метода противостояния кибервызову дается с трудом. Процесс осложняется наличием значительных различий между ядерным оружием и оружием кибервойны: проблемами и ограничениями кибероборонны и контроля над вооружениями, вероятной потребностью в междоменной стратегии сдерживания/возмездия (в которой может учитываться или не учитываться фактор ядерного оружия), изначально существующими трудностями атрибуции и неясностью характера и масштаба любой будущей киберугрозы или атаки. Эти переменные величины и превращают выработку национальной ядерной киберстратегии в непростую и проблемную задачу.

Кибероружие часто сравнивают с ядерным, но это совершенно разные вещи. Между ними, по крайней мере, четыре пункта различия: масштаб и характер угрозы, типы целей, участвующие акторы, а также правила и конвенции, регулирующие их использование. Что касается масштаба, то даже самые изощренные кибератаки не причинят таких же разрушений, какие способна причинить (и причиняла) ядерная бомба. К тому же, кибероружие едва ли можно назвать стратегическим. Отчасти – потому что у кибератак и ядерных ударов разные цели. Хотя ядерный удар и может быть ограниченным и узконаправленным, ядерное оружие как таковое считается средством неизбирательного действия, способным причинить огромные разрушения. При этом даже самые грозные кибератаки являются специализированными и направленными на определенные цели акциями, для которых зачастую требуется заведомое знание цели.

Хотя киберугроза и отличается от угрозы, создаваемой ядерным оружием, государствам, тем не менее, необходимо хорошо поразмыслить над тем, как защищаться от кибератак, предотвращать их, и в дальнейшем наносить ответный удар. Но кибербезопасность и кибероборона, более широкое понятие сдерживания на основе отказа в доступе и концепция контроля над кибервооружениями по-прежнему остаются проблематичными. Поэтому в любую стратегию следует включить концепцию сдерживания на основе наказания и угрозы возмездия.

Однако для предотвращения кибератак с помощью угрозы наказания требуется знать, можно ли с уверенностью установить источник атаки, и какую форму должна иметь ответная реакция, чтобы стать действенной, пропорциональной и законной. Есть и другой вопрос: должно ли кибероружие рассматриваться отдельно или как часть более широкой (междоменной) стратегии сдерживания, включающей другие формы военной и политической мощи? Дело еще больше осложняется тем, что концепцию сдерживания, возможно, придется приноравливать к специфическим типам атак, учитывая широкое разнообразие разновидностей деятельности, попадающих в разряд кибератак.

Если сдерживание кибератак должно быть приспособлено к специфическим типам угрозы и нападения, то возникает проблема, связанная с выбором варианта реагирования. Не исключено, что некоторые типы кибератак потребуют асимметричного ответа, в том числе, с использованием подвижных военных сил. Поэтому кибероружие, возможно, придется включить в междоменное планирование операций сдерживания. Подобного рода рассуждения с неизбежностью приводят к рассмотрению вопроса о том, есть

ли вообще какая-либо возможность найти место для ядерного оружия в иерархии средств сдерживания в случае кибератаки, угрожающей жизненно важным центрам государства.

Безусловно, во включении ядерных сил в междоменную стратегию киберсдерживания есть определенная логика. Но большинство аналитиков ставят под вопрос целесообразность смешения ядерного и кибероружия, так как кибератаки не грозят такими разрушениями и поражением жизненно важных центров, как атака ядерная. Нанесение ядерного удара в ответ на кибератаку является действием непропорциональным и неоправданным, а киберсдерживание трудно осуществлять на практике. Более того, объединение обоих типов оружия дает новую мотивацию сторонникам распространения ядерного оружия[29]. Учитывая нынешний масштаб киберугрозы, использование ядерного оружия для борьбы с кибероружием и его сдерживания удачным вариантом не представляется. Однако при изменении характера угрозы ядерное оружие, вероятно, еще сможет сыграть определенную роль в будущем.

Заключение

В ближайшем будущем кибероружие в качестве абсолютного символа и гарантии национальной безопасности не сможет заменить ядерное. Не будет оно представлять и стратегической или экзистенциальной угрозы. Но эти средства все же знаменуют собой важный сдвиг в том, что мы думаем о ядерном оружии и ядерной безопасности и как улаживаем отношения в этой сфере и блюдем ядерную стабильность, регулируем мировой ядерный порядок. Появление и распространение кибернетических средств нападения изменяет, переиначивает и усугубляет характер нынешней напряженности в пределах всей области ядерных вооружений. Появляются новые динамические составляющие и новые вызовы, которые необходимо понять и освоить.

Киберугрозы, кроме того, будут иметь и более масштабные последствия. Осознание того, что ядерные системы могут быть повреждены, подвергнуться нападению и перестать функционировать в штатном режиме, может привести к модернизации ядерных сил и распространению ядерного оружия, повлиять на существующие соглашения о контроле над ядерными вооружениями и на ядерные режимы, и стать новым препятствием на пути сокращения этого вида вооружений. Особенно тревожным представляется сочетание кибертехнологий с другими потенциально дестабилизирующими средствами – это способно подорвать стратегическую стабильность, повысить вероятность вмешательства третьих сторон и умножить шансы неверной оценки ситуации и даже использования ядерного оружия.

---

[29] *Timothy Farnsworth, "Is there a place for nuclear deterrence in cyberspace?", Arms Control Now, (30 мая 2013 г.), http://armscontrolnow.org/2013/05/30/is-there-a-place-for-nuclear-deterrence-in-cyberspace/.*

Легких путей разрешения этой проблемы не существует. Начинать же надо с начала: разобраться в характере вызова и прийти к относительному согласию о значении самого термина. Вторая рекомендация обращена ко всем ядерным державам, которым необходимо надежно защитить свои ядерные системы от кибератак. Им также нужно принять меры по минимизации последствий кибервмешательства: усовершенствовать системы и создать запасные, улучшить подготовку и подбор операторов, отработать время применения оружия. Все это можно делать совместно и положить в основу моратория или межгосударственных соглашений о взаимном неприменении кибероружия против ядерных систем. И хотя мир не застрахован от вероятности нападения третьих сторон, надо использовать шанс для создания основы доверия и сотрудничества. Наконец, кибероружие, наравне с другими современными стратегическими средствами, должно стать предметом обсуждения в контексте ядерного дискурса, предметом диалога и соглашений о контроле над вооружениями.

Эта записка заимствует идеи, впервые опубликованные на английском языке как "Cyber threats and nuclear weapons", RUSI Occasional Paper, (июль 2016), https://rusi.org/publication/occasional-papers/cyber-threats-and-nuclear-weapons-new-questions-command-and-control. (исследование подготовлено на основании гранта Британского Совета экономического и социального развития № ES/K008838/1).

#Valdaiclub

ValdaiClubRu
https://twitter.com/ValdaiClubRu

ValdaiClubRu
https://www.facebook.com/ValdaiClubRu/

ru.valdaiclub.com

valdai@valdaiclub.com

СОВЕТ ПО ВНЕШНЕЙ И ОБОРОННОЙ ПОЛИТИКЕ

РСМД
Российский совет
по международным
делам

МГИМО
УНИВЕРСИТЕТ

ВЫСШАЯ ШКОЛА ЭКОНОМИКИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ