Валдайские записки

Валдай | Международный дискуссионный клуб

№ 95

Необходимость запрета кибератак в ядерной сфере и превентивные меры США и России в сфере контроля над вооружениями

Эндрю Фаттер

ru.valdaiclub.com
#valdaiclub

Ноябрь, 2018

Об авторе

Эндрю Фаттер
Доцент Департамента политики и международных отношений
Университета Лестера, Великобритания

Данный текст и другие материалы
можно найти на нашем сайте:
http://ru.valdaiclub.com/a/valdai-papers/

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

© Фонд развития и поддержки Международного
дискуссионного клуба «Валдай», 2018

Российская Федерация, 115184, Москва,
улица Большая Татарская, дом 42

Введение: киберугрозы для ядерных объектов

Рональд Рейган в годы своего президентства обычно посвящал воскресный вечер просмотру фильмов. И вот, около 35 лет назад он решил посмотреть вышедший тогда в прокат голливудский блокбастер «Военные игры» («WarGames») с Мэттью Бродериком в главной роли. В фильме рассказывается о юном хакере, которому случайно удаётся взломать сверхсекретные суперкомпьютеры Пентагона, которые контролируют американский ядерный арсенал. В результате США оказываются на грани (воображаемой) Третьей мировой войны против Советского Союза с использованием ядерного оружия. Этот фильм настолько поразил Рейгана, что он распорядился провести секретную проверку, чтобы оценить, насколько ядерное оружие США уязвимо перед лицом сетевых атак[1], и могут ли хакеры посредством компьютерного взлома осуществить пуск носителей с ядерными боезарядами в обход официального Вашингтона. В результате выяснилось, что такая угроза реально существует, при этом её степень гораздо выше, чем ожидали эксперты[2]. Так, благодаря фильму 1983 г., впервые возникло понимание, что ядерные объекты и системы могут быть уязвимы перед лицом кибератак.

Поколение спустя эта угроза существенно выросла. Всё больше элементов ядерной инфраструктуры — от боеголовок и средств их доставки до систем управления и наведения — сильнее зависят от сложного программного обеспечения, что делает их потенциальными мишенями для атак. Более того, все ядерные державы занимаются модернизацией своих систем ядерного оружия, при этом стремясь внедрять компьютерные технологии, активнее использовать сетевые решения и возможности программирования. В то же время, растёт и осознание угрозы, которую представляют хакеры для всех компьютерных систем, в том числе для критически важных объектов национальной инфраструктуры. Самым известным примером стала, пожалуй, обнаруженная в 2010 г. кибератака с использованием компьютерного червя Stuxnet против ядерного центра по обогащению урана в иранском городе Натанз. Между тем кибератаки происходят постоянно, став объектом пристального внимания для органов военного планирования. Так, в большинстве стран в рамках вооружённых сил созданы специализированные подразделения и приняты доктрины по вопросу о наступательных кибероперациях, а в некоторых документах упоминаются даже

[1] *Подробнее на эту тему читайте в недавней книге автора: Futter, A, 2018, 'Hacking the Bomb', Georgetown University Press. URL: http://press.georgetown.edu/book/georgetown/hacking-bomb*

[2] *Kaplan F. 'WarGames' and Cybersecurity's Debt to a Hollywood Hack // The New York Times. 2016. February 19. URL: https://www.nytimes.com/2016/02/21/movies/wargames-and-cybersecuritys-debt-to-a-hollywood-hack.html*

кибервойны. Таким образом, в современном мире ядерные арсеналы всех стран, имеющих такое оружие, уязвимы перед лицом кибератак. Этот факт, в частности, был признан в докладе Научного совета Министерства обороны США в 2013 г.[3]

Хорошая новость заключается в том, что эта угроза появилась сравнительно недавно и пока находится в зачаточном состоянии, а это значит, что ещё есть время принять упреждающие меры, чтобы по возможности смягчить или устранить её наиболее опасные аспекты до того, как они проявятся в полную силу и станут нормой. Проблема заключается в том, что российско-американские отношения в настоящее время достигли своей низшей точки со времён Холодной войны, что заметно снижает возможность достижения договорённостей между двумя странами по вопросу о контроле над вооружениями. При этом обе стороны (а, возможно, и другие государства) активно ищут способы взломать системы ядерного оружия друг друга. Автор данной статьи выступает с призывом возобновить сотрудничество в ядерной сфере и ввести мораторий на кибератаки против ядерных объектов и систем, который бы охватывал США и Россию, а также по возможности и ряд других стран. Как будет показано далее, если хакеры не будут пытаться вмешиваться в работу систем управления ядерным оружием, это пойдёт на пользу всем без исключения странам — и всему населению земного шара.

Становление нормы

Процесс включения компьютерных сетевых операций (более точный термин по сравнению с приставкой «кибер»[4]) в программы военного планирования был запущен как минимум 30 лет назад и чётко прослеживается по меньшей мере с конца 1980-х гг. и так называемой революции в военном деле начала 1990-х гг. Однако эти идеи вместе с соответствующими технологиями приобрели актуальность с точки зрения стратегического планирования в области ядерных вооружений лишь в последнее десятилетие или около того. В этой связи необходимо отметить сформулированные в начале 2000-х гг. планы администрации Джорджа Буша-младшего по диверсификации программ ядерного сдерживания за счёт повышения роли неядерных средств в глобальной ударной системе вооружений, а также решение использовать киберсредства против иранской ядерной программы, а затем

[3] *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat. United States Department of Defense, Defense Science Board. January 2013. URL: http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf*

[4] *См.: Futter A. Cyber Semantics: Why we Should Retire the Latest Buzzword in Security Studies // Journal of Cyber Policy. 2018. URL: https://www.tandfonline.com/doi/full/10.1080/23738871.2018.1514417*

и недавние предложения Пентагона по созданию системы «противоракетной обороны полного спектра» и комплексов быстрого глобального удара.

Идея системы «противоракетной обороны полного спектра» достаточно проста и заключается в расширении комплекса традиционных средств противоракетной обороны, включая основанные на технологии кинетического перехвата системы ПРО, за счёт новых методов предупреждения запуска ракет. Суть заключается в том, чтобы предотвратить сам запуск посредством вмешательства в работу основных систем управления или функционирования самого орудия электронными (провоцирование сбоя в работе телеметрии) или цифровыми средствами (повреждение программного, аппаратного обеспечения или системы поддержки). Для этого хакерам нужно взломать системы управления ядерным оружием ещё до запуска ракет, заразить системы ракеты или связанных с ней объектов инфраструктуры вредоносным кодом или иным образом создать помехи для функционирования таких систем. Такая тактика называется «блокированием пуска» (left-of-launch).

Теоретически, сочетание кинетических и некинетических методов противоракетной обороны позволяет придать системе обороны комплексный характер и снижает её зависимость от возможности перехвата ракеты в воздухе, что даже в современных условиях остаётся весьма непростой задачей[5]. Старший помощник заместителя министра обороны США по вопросам политики Брайан МакКеон в ходе выступления на слушаниях в Конгрессе США в 2016 г. отметил: «Нам нужно разработать более широкий набор средств, который бы включал меры по блокированию угроз до осуществления пуска. Разработка таких решений по предотвращению запуска ракет дала бы командованию США дополнительные средства и возможности в области противоракетной обороны. Это, в свою очередь, позволило бы снизить нагрузку на системы перехвата баллистических ракет. Сочетание систем блокирования пуска и перехвата ракет позволит повысить эффективность и стойкость систем противоракетной обороны перед лицом возможного запуска баллистических ракет противником»[6].

Наиболее очевидной целью для такой системы противоракетной обороны полного спектра могла бы стать Северная Корея. Не исключено, что американские хакеры внесли свой вклад в провал ряда недавних

[5] *См., например: Larter D. Reality Check: Failures Happen, Even in Missile Defense Testing // Defense News. 2018. February 1. URL: https://www.defensenews.com/naval/2018/02/01/reality-check-failures-happen-even-in-missile-defense-testing/*

[6] *McKeon B.P. Statement before the Senate Armed Services Subcommittee on Strategic Forces. April 13, 2016. URL: http://www.armed-services.senate.gov/imo/media/doc/McKeon_04-13-16.pdf.*

ракетных испытаний[7]. Вероятно, у США имеются аналогичные планы в отношении Ирана на случай создания страной ядерного оружия. Кроме того, администрация Трампа может включить в свой следующий «Обзор противоракетной обороны» (Missile Defense Review) отсылку к комплексным возможностям «полного спектра» в дополнение к модернизации существующих систем.

Значимым моментом последних двух десятилетий в сфере противоракетной обороны является появление высокоточного удара. И в сфере военного и ядерного планирования грань между обороной и нападением стала размытой. Можно даже сказать, что происходит постепенный отход от идеи сдерживания за счёт взаимной уязвимости — принципа, который лежит в основе доктрины взаимного гарантированного уничтожения. При этом наблюдается переход к более активным мерам обороны и сдерживания. Эти изменения вызваны в первую очередь переменами внутри «стороны спроса» (объекта, в отношении которого должно проводиться сдерживание) на усиление ядерного сдерживания. Другими словами, если раньше речь шла о предотвращении массированного ядерного удара со стороны соперника сопоставимой мощи, то теперь необходимо сначала определить, в отношении кого или чего и как проводить политику сдерживания, поскольку ядерная угроза может исходить и от более мелких «государств-изгоев», не признающих международных норм, и даже от террористов, которые не придерживаются общепринятых правил и ведут себя не столь рационально, как крупные державы-соперники.

Однако в настоящее время снова произошли сдвиги, теперь благодаря динамике «предлагающей стороны» (стороны, которая реализует сдерживание) в области ядерного сдерживания с учётом стремительного технического прогресса и развития систем вооружений на волне недавней революции в сфере информационных и компьютерных технологий. Наилучший тому пример — цифровое оружие, компьютерные сетевые технологии и другие средства, которые можно характеризовать приставкой «кибер». К таким средствам также относятся и другие виды перспективного неядерного оружия, которые могут дополнить, а в некоторых случаях и заменить ядерное оружие с точки зрения стратегического планирования. В результате, в дополнение к сдерживанию за счёт неминуемого ответного удара, а может и в обход этому принципу, растёт интерес к сдерживанию посредством блокирования использования наступательных средств (то есть предотвращения атаки).

---

[7] *Sanger D.E., Broad W. Trump Inherits Secret Cyberwar Against North Korean Missiles // The New York Times. 2017. March 4. URL: https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html*

Новые проблемы и тенденции

Проблема заключается в том, что в отличие от систем кинетического перехвата баллистических ракет, которые нужно разворачивать, можно увидеть и сосчитать, киберсредства блокирования удара по своей природе невидимы и даже эфемерны. Неудивительно, что Москва и Пекин испытывают беспокойство в связи с развитием таких средств, опасаясь, как и в случае с неядерными системами противоракетной обороны, возможности их использования в будущем против себя. Отличие этих систем в том, что нет возможности оценить масштаб такого рода угрозы и соответственно реагировать (наращивать арсенал ракет, развивать новые средства преодоления ПВО и т.д.) для сохранения стратегического паритета или, по крайней мере, предотвратить получение одной стороной (в данном случае США) стратегического преимущества или даже превосходства.

Например, 44 американских комплекса ракет-перехватчиков наземного базирования, размещённых на Аляске и в Калифорнии (даже в сочетании с системами противоракетной обороны в других регионах), едва ли представляют на данный момент угрозу для России или Китая с точки зрения возможности нанесения ими гарантированного ответного удара. Однако ситуация может измениться в случае существенного наращивания количества перехватчиков и необходимых для их работы локаторов при сокращении ядерного потенциала России и сохранении китайского арсенала в текущих размерах. Однако и Россия, и Китай не могут не отреагировать на такие изменения в стратегическом балансе. Скорее всего, они уже предпринимают ответные действия, разрабатывая новые средства преодоления систем противоракетной обороны, чтобы предотвратить изменение баланса в пользу США[8].

Между тем оценить масштаб угрозы и выработать адекватный ответ очень трудно, учитывая призрачный и неосязаемый характер технологий блокирования удара до пуска. Кроме того, в то время как системы противоракетной обороны, работающие по принципу кинетического перехвата, разрабатывались для борьбы с ракетами наземного базирования, возможность проведения атак против центральных командных пунктов (и систем раннего

[8] *Roth A. Putin Threatens US Arms Race with New Missile Declaration // The Guardian. 2018. March 1. URL: https://www.theguardian.com/world/2018/mar/01/vladimir-putin-threatens-arms-race-with-new-missiles-announcement*

предупреждения) делает все системы ядерного оружия уязвимыми. Кибератаки могут быть направлены даже против подводных крейсеров, оснащённых ядерным оружием, и подвижных ракетных комплексов, которые играют ключевую роль в обеспечении возможности нанесения Россией и США гарантированного ответного удара. В результате очевидно, что реализация политики комплексной противоракетной обороны «полного спектра» не может не вызвать обеспокоенность у стратегических соперников США, тем самым повышая уровень неопределённости[9].

В отношении такой комплексной системы противоракетной обороны «полного спектра» существует ещё целый ряд проблем, которые заслуживают особого внимания. Во-первых, придание приоритетного значения средствам блокирования пуска для преодоления угроз ракетного или ядерного удара меняет суть противоракетной обороны и в целом политики безопасности. На смену во многом пассивной позиции приходит превентивный подход, поскольку система должна быть взломана до того, как угроза пуска станет совершенно очевидной, и совершенно определённо до непосредственного запуска ракеты. Такая ситуация называется «активной обороной»: хакеры должны взломать соответствующие системы до того момента, когда ракета может быть запущена. Это может подразумевать вмешательство на этапе производства или смещение фокуса в сторону человеческого фактора. Безусловно, некоторые действия можно предпринять после начала подготовки ракеты или иного средства доставки ядерной боеголовки к запуску, однако для большей уверенности в желаемом исходе такой операции хакерам наверняка нужно будет заранее получить возможность обойти систему защиты или заразить её вирусом.

Во-вторых, сама возможность наличия в системах ядерного оружия уязвимостей для хакеров и их нештатного срабатывания подрывает доверие и стабильность в отношениях между ядерными державами. Пониженная определённость в работе таких систем может подтолкнуть страны к действиям по обеспечению максимального контроля над ядерным оружием, то есть к гарантированию его срабатывания, возможно, в ущерб их сохранности и безопасности. Кроме того, другие также поспешат обзавестись средствами блокирования пуска ракет, что заставит все страны чувствовать себя в меньшей безопасности вне зависимости от того, собираются ли они действительно их использовать. Распространение чувства страха на международной арене вряд ли будет способствовать достижению каких-либо договорённостей в области контроля над вооружениями как в двухстороннем, так и многостороннем форматах.

---

[9] *См. подробнее: Futter A. The Dangers of Using Cyberattacks to Counter Nuclear Threats // Arms Control Today. 2016. July/ August. URL: https://www.armscontrol.org/print/7551*

В-третьих, повышается риск аварий и непредвиденных происшествий, возникающих как в связи со взломом не тех систем, так и с обнаружением взлома. Например, средства управления неядерным оружием или системами поддержки (например спутниками) могут также использоваться для управления системами ядерного оружия или распространяться на них. Аналогичным образом, можно предположить, что, проникнув в эти системы, хакеры могут спровоцировать непредвиденный ими или непреднамеренный эффект. Кроме того, сложно с точностью установить намерения хакера или вредоносной программы, обнаруженной внутри сети (и определить их происхождение). В таком случае жертва может оказаться в наиболее неблагоприятной ситуации, особенно если атака разворачивается в период высокой напряжённости. Обнаружение такого взлома может спровоцировать цепную реакцию, стать причиной обострения дипломатических противоречий, а сам взлом — быть воспринятым как акт агрессии.

Наконец, существует также возможность возникновения или обострения кризисной ситуации со стороны третьих сил, например террористов, за счёт проведения провокационных атак против компьютерных систем управления ядерным оружием. При этом такие силы с гораздо большей вероятностью будут стремиться провести против ядерных систем «активирующие» действия, тогда как для государств главная цель заключается в том, чтобы «дезактивировать» эти системы. Такие группы могут попытаться спровоцировать подачу сигнала тревоги системами раннего предупреждения и манипулировать информационными системами или создать хаос посредством относительно незначительных провокационных вылазок, якобы осуществлённых государством-противником. Очевидно, что реализация любого такого сценария может привести к эскалации и повышению риска инцидента с использованием ядерного оружия.

На данный момент идеей использования цифровых средств для взлома систем управления ядерным оружием и ракетами преимущественно занимаются в США (до недавнего времени ситуация обстояла аналогичным образом с технологией кинетического перехвата). Однако другие страны могут последовать их примеру. Получить возможность влиять на работу аналогичных систем США могут Россия, Китай и, возможно, другие страны, что повысит риски для всех вовлечённых сторон. При этом не исключено, что США даже более уязвимы, учитывая широкое применение сложных систем в управлении ядерной инфраструктурой, а также планы по модернизации всех составляющих систем управления и контроля[10].

---

[10] *Futter A. The Double-Edged Sword, US Nuclear Command and Control Modernisation // Bulletin of the Atomic Scientists. 2016. June 29. URL: https://thebulletin.org/2016/06/the-double-edged-sword-us-nuclear-command-and-control-modernization/*

Работа на опережение

Простого решения этой сложной проблемы не существует. В истории мало примеров успешного предотвращения негативных последствий использования новых технологий в военных целях в качестве превентивной меры их применения в полную силу. Кроме того, на современном этапе достижение США и Россией каких-либо договорённостей по контролю над вооружениями представляется маловероятным, хотя недавняя встреча между Дональдом Трампом и Владимиром Путиным в Хельсинки вселяет некоторую надежду[11]. Однако возможность снизить риск наиболее тревожных последствий киберугрозы в сфере ядерного оружия до того, как она выйдет из-под контроля, всё-таки существует. Необходимо начать с обсуждения наиболее острых для обеих сторон вызовов. Очевидно, что отправной точкой могла бы стать проблема хакеров, пытающихся взломать системы управления ядерными вооружениями, под контролем которых находятся сотни ракет. Впоследствии это позволило бы перейти к обсуждению других инициатив, представляющих взаимный интерес.

Первой такой темой могло бы стать согласование новых ограничений в использовании компьютерных сетевых операций в отношении систем ядерного оружия и формулирование определённых «правил игры» в этой сфере. Так можно было бы избежать некоторых угроз, договорившись о новых формах контроля над вооружениями в этой области, в частности путём заключения соглашения об отказе от атак против имеющихся у обеих сторон систем ядерного оружия с использованием таких средств. Такого рода договорённость не обязательно должна быть оформлена, как прежние договоры по ядерным вооружениям. Для начала США и Россия могли бы выступить с заявлением, в котором они бы признали серьёзность и рискованность атак против систем управления ядерным оружием и взяли бы на себя обязательство не прибегать к такому варианту действий. Затем в декларативном порядке можно было бы зафиксировать: (1) как такие атаки будут восприниматься и каким будет вероятный ответ в случае обнаружения таковых действий, и (2) что системы ядерного оружия не должны быть мишенью таких атак. В дальнейшем можно было бы распространить эти принципы и на другие ядерные державы. В основе этого лежала бы та же логика, что и при заключении Договора об ограничении систем противоракетной

[11] *Bender B. Leaked Document: Putin Lobbied Trump on Arms Control // Politico. 2018. July 8. URL: https://www.politico.com/story/2018/08/07/putin-trump-arms-control-russia-724718*

обороны 1972 г., который подразумевал ограничение таких систем в целях повышения предсказуемости и стабильности в отношениях между соперничающими ядерными державами. Очевидно, что в такой ситуации невозможен контроль традиционными средствами, как невозможно предотвратить подобные действия со стороны негосударственных игроков. Но это стало бы началом. Государства будут менее склонны пойти на риск быть пойманными на нарушении заявленной политики или взятых на себя обязательств.

Второй областью взаимодействия могло бы стать повышение безопасности, содействие регулированию и сотрудничеству в этой сфере. Начать можно было бы в одностороннем порядке посредством, например, сокращения продолжительности нахождения ядерных систем в активном режиме готовности (для снижения возможности хакеров, представляющих негосударственные субъекты, спровоцировать пуск или взрыв), принятия мер по обеспечению независимости таких систем от других неядерных вооружений и систем управления (для снижения риска случайной, непреднамеренной активации не тех систем в ходе атаки) и обеспечения простоты инфраструктуры системы управления и контроля (чтобы её работа была понятна и за счёт этого менее уязвима для хакерских атак). Всё это могло бы создать предпосылки для реализации более масштабных двухсторонних и даже многосторонних мер по повышению доверия. Страны, в первую очередь Россия и США, а затем, возможно, и другие государства, могли бы обмениваться передовым опытом, а также данными об угрозах, исходящих от негосударственных субъектов, и даже создавать группы с участием высоких должностных лиц и других стейкхолдеров для поиска оригинальных решений применительно к новым механизмам контроля над вооружениями. Кроме того, может быть создан совместный международный центр раннего предупреждения и оценки угроз для поддержания постоянного диалога между официальными лицами и экспертами и обеспечения возможности оперативного реагирования при возникновении угроз со стороны третьих сил или вопросов, требующих безотлагательных действий.

Сейчас перед нами открывается возможность предвосхитить серьёзный сдвиг в сфере международной ядерной политики, который чреват негативными последствиями для всех ядерных держав, а значит и для всех нас. Необязательно чтобы новые договорённости по контролю над вооружениями походили на договоры прошлых лет или подразумевали оперативную разработку и реализацию соответствующих мер. Главное, чтобы такие договорённости были достигнуты. На кодификацию ядерной революции ушло почти два десятилетия, и с тех пор процесс уточнения сформулированных тогда норм продолжается. Наши действия по предупреждению ядерных

угроз нового поколения должны включать инновационные подходы в сфере контроля над вооружениями и политики сдерживания, а также, возможно, новые правила вкупе с полным осознанием угрозы и желанием действовать на многосторонней основе.

В конечном счёте, необходимо будет учитывать угрозы, исходящие от новых, пока «экзотичных» технологий в сфере ядерных вооружений при обсуждении вопросов стратегической стабильности, заключении соглашений по контролю над вооружениями и в рамках более широких инициатив по нераспространению и разоружению. В современном мире обсуждение ядерной проблематики не может происходить в технологическом вакууме. Нельзя больше игнорировать очевидную связь между ядерными и неядерными вооружениями. Соответственно, нам следует признать, что свершившаяся недавно революция в области информационных и компьютерных технологий, развитие систем противоракетной обороны, появление высокоточных вооружений, беспилотных летательных аппаратов, противокосмических вооружений, искусственного интеллекта, а также киберугроз привели к изменению международной обстановки в сфере ядерных вооружений, что требует от нас новых подходов к управлению ядерным оружием и обеспечению его сохранности.

Заключение: упреждающие меры по контролю над вооружениями

Вместо того, чтобы выступать с опрометчивыми и опасными заявлениями по вопросам, связанным с ядерным оружием, и тратить огромные суммы денег на разработку всё более разрушительных видов вооружений, президентам Трампу и Путину и/или их представителям следовало бы сесть за стол переговоров и серьёзно обсудить основные риски, с которыми сталкиваются их страны в сфере ядерного оружия. Естественно, что по всем вопросам им не удастся достичь соглашения. Однако взаимное признание того, что хакерские атаки против систем ядерного оружия друг друга никому на пользу не пойдут, было бы хорошей отправной точкой. Можно предположить, что развитие диалога по вопросу о контроле над вооружениями в таком ключе было бы куда более плодотворным, чем текущие переговоры в логике Договора о сокращении стратегических наступательных вооружений. Возможно, вместо обсуждения сокращения вооружений можно было бы, хотя бы временно, сконцентрироваться на необходимости избегать

его применения. Это бы напомнило тем, кто считает, что контроль над вооружениями утратил актуальность[12] или невозможен в киберпространстве, что есть и другие способы обеспечения стабильности, которые необязательно должны воспроизводить подходы прошлых лет. Урок Холодной войны заключается в том, что даже если достижение каких-либо договорённостей по ядерным вооружениям казалось маловероятным, обе стороны осознавали необходимость продолжения диалога, понимая, что на кон поставлено слишком многое.

В дальнейшем этому процессу следует придать многосторонний характер, ведь в отличие от ядерных угроз времён Холодной войны, теперь действующих сил уже не две, а гораздо больше. Это касается не только всех государств, обладающих ядерным оружием, но и всех сил, обладающих возможностью проведения кибератак. Вместо попыток заключения всеобъемлющего договора или широкомасштабной договорённости по кибербезопасности в ядерной сфере, можно было бы в качестве первого шага начать с разработки конвенции по использованию кибертехнологий применительно к ядерному оружию или, как минимум, каких-то общих правил[13]. В первую очередь необходимо установить и согласовать используемую терминологию для понимания, что именно каждая из сторон подразумевает под термином «ядерный». Это позволило бы заложить основу для обсуждения такой проблематики на международных форумах, а также в рамках более общих дискуссий по вопросу о контроле над вооружениями. Глобальная система регулирования ядерного оружия находится состоянии неопределённости и, вероятно, переживает переходный период, что во многом стало результатом появления множества новых технологических возможностей на волне революционного скачка в развитии информационных и компьютерных технологий.

Когда-то для наращивания военного потенциала нужно было строить новые объекты или производить вооружения, что, как правило, требовало огромных затрат, а угрозы, исходящие от новых видов вооружений, становились реальностью ещё до заключения соглашений, направленных на устранение таких угроз. Однако, учитывая современный технологический

---

[12] *Rumer E. A Farewell to Arms… Control // Carnegie Endowment for International Peace, US-Russia Insight. 2018. April 17. URL: https://carnegieendowment.org/2018/04/17/farewell-to-arms-.-.-.-control-pub-76088; Arbatov A. An Unnoticed Crisis: The End of History for Nuclear Arms Control // Carnegie Moscow Center. 2016. March 16. URL: http://carnegie.ru/2015/03/16/unnoticed-crisis-end-of-history-for-nuclear-arms-control-pub-59378*

[13] *См., например: Statement by the Euro-Atlantic Security Leadership Group, Support for Dialogue Among Governments to Address Cyber Threats to Nuclear Facilities, Strategic Warning and Nuclear Command and Control. 2018. February 16. URL: https://www.europeanleadershipnetwork.org/wp-content/uploads/2018/02/Cyber-Statement-Feb-16-Final-Text.pdf*

и политический контекст, такая логика может стать для нас фатальной. Если бы мы могли прийти к общему пониманию тех угроз, которых наши общества и страны хотели бы избежать, можно было бы совместными усилиями создать механизмы для их предупреждения и устранения. Определённо, мы все согласны, что хакеры, «орудующие» в системах управления готовым к запуску ядерным оружием, а также страх, что ядерное оружие может не сработать или же быть запущено террористами — это одинаково плохо для всех.

СОВЕТ ПО ВНЕШНЕЙ И ОБОРОННОЙ ПОЛИТИКЕ

РСМД
Российский совет
по международным
делам

МГИМО
УНИВЕРСИТЕТ

ВЫСШАЯ ШКОЛА ЭКОНОМИКИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

ValdaiClubRu
ValdaiClubRu
t.me/valdaiclub
ValdaiClub
valdaiclubcom
valdai@valdaiclub.com