ЯДЕРНОЕ ОРУЖИЕ В НОВОЮ КИБЕР-ЭПОХУ

Доклад Аналитической группы по изучению киберугроз безопасности ядерных вооружений

СЕНТЯБРЬ 2018 Г.

Авторы: д-р Пейдж Стаутлед и Саманта Питтс-Кифер

Предисловие: Эрнест Мониз, Сэм Нанн, Дес Браун

NTI
BUILDING A SAFER WORLD

Об Аналитической группе по изучению киберугроз безопасности ядерных вооружений

В 2016 году Инициатива по сокращению ядерной угрозы (NTI) создала Аналитическую группу высокого уровня по изучению киберугроз безопасности ядерных вооружений для определения кибер-уязвимостей, присущих ядерным вооружениям, а также разработки рекомендаций по устранению таких уязвимостей и минимизации потенциальных последствий кибератак. Членами Группы являются бывшие и вышедшие в отставку правительственные чиновники высокого уровня, военные руководители и специалисты по системам ядерных вооружений и политике их применения. На первом этапе проекта основное внимание уделялось уязвимостям американского ядерного оружия. Аналогичная проблематика применительно к иностранным ядерным вооружениям будут изучаться на следующих этапах. Список участников Группы приведен в конце данного доклада.

В ходе первого этапа Группа провела два заседания. В сентябре 2016 года члены Группы признали, что киберугроза является предметом обоснованных опасений, и приступили к определению типов систем и атак, которые могут представлять угрозу для ядерных вооружений и привести к серьезным последствиям. В июне 2017 г. Группа проанализировала четыре вероятных сценария атак, нацеленных на ядерные вооружения и способных привести к наиболее разрушительным последствиям.

Группа предоставила NTI экспертные комментарии по содержанию проекта доклада и содержащимся в нем рекомендациям. Участие в Группе не подразумевает согласия со всеми аспектами доклада и его рекомендациями.

Об Инициативе по сокращению ядерной угрозы (NTI)

Усилия Инициативы по сокращению ядерной угрозы (NTI) направлены на защиту жизни и здоровья людей, охрану окружающей среды и обеспечение качества жизни нынешнего и будущего поколений. Мы работаем над предотвращением катастрофических атак с использованием оружия массового поражения и дезорганизации (ОМПД). Инициатива была основана в 2001 году бывшим американским сенатором Сэмом Нанном и филантропом Тедом Тернером, которые и поныне являются ее сопредседателями. Руководство работой Инициативы осуществляется Советом директоров, в который входят известные деятели из нескольких стран мира. Эрнест Мониз является исполнительным директором и сопредседателем, Дес Браун вице-председателем, а Джоан Ролфинг – президентом NTI.

www.nti.org

ЯДЕРНОЕ ОРУЖИЕ В НОВОЮ КИБЕР-ЭПОХУ

Доклад Аналитической группы по изучению киберугроз безопасности ядерных вооружений

СЕНТЯБРЬ 2018 Г.

Авторы: д-р Пейдж Стаутлед и Саманта Питтс-Кифер

Предисловие: Эрнест Мониз, Сэм Нанн, Дес Браун

NTI
BUILDING A SAFER WORLD

Взгляды, изложенные в данной публикации, могут не отражать взглядов Совета директоров NTI и организаций, с которыми они связаны.

Изображение на обложке (сверху): U.S. General Services Administration
Изображение на обложке (снизу): Zenobillis for Shutterstock

Содержание

Благодарности

Авторы выражают благодарность сопредседателю и исполнительному директору Инициативы по сокращению ядерной угрозы (NTI) Эрнесту Монизу, сопредседателю NTI Сэму Нанну и вице-председателю Десу Брауну за их неустанные усилия по сокращению ядерной угрозы и создание Аналитической группы по изучению киберугроз безопасности ядерных вооружений. Мы также благодарны Президенту NTI Джоан Ролфинг за ее неоценимый вклад в данный проект. Руководство NTI вовремя осознало актуальность проблемы киберугроз, направленных против ядерных вооружений и связанных с ними систем. Его помощь и интеллектуальное содействие внесло огромный вклад в успех данного проекта.

Авторы также глубоко признательны членам Аналитической группы по изучению киберугроз безопасности ядерных вооружений, в которую входят наиболее авторитетные гражданские и военные специалисты из США и других стран. Мы благодарны членам Группы за время, уделенное ее работе; мы постарались наиболее полным образом отразить их взгляды в данном докладе.

Кроме того, авторы хотели бы поблагодарить Совет директоров NTI за оказанную поддержку. Мы особо признательны финансовым донорам, в т.ч. Фонду МакАртуров и Корпорации Карнеги, за поддержку данного проекта.

Наконец, мы в долгу перед нашими коллегами по NTI за их вклад не только в работу по киберугрозам безопасности ядерных вооружений, но и в подготовку данного доклада. В частности, мы благодарны членам Отдела коммуникаций NTI Мими Холл и Кармен МакДугал. Мы бы также хотели выразить признательность Стиву Андреасену, Катерин Крэри, Эрин Дамбахер, Брайану Роузу и Линн Растен за их значительный вклад в проект, а также Хоуп Фашинг, Мэри Фулэм, Джулии Хейбигер, Андреасу Павлоу, Александре Ван Дайн и Маргарет Вильямс за их дополнительную поддержку.

Д-р Пейдж Стаутленд
Вице-президент
по научно-техническим вопросам
Инициатива по сокращению
ядерной угрозы (NTI)

Саманта Питтс-Кифер
Старший директор
Программа глобальной ядерной политики
Инициатива по сокращению ядерной
угрозы (NTI)

ПРЕДИСЛОВИЕ

сопредседателей Аналитической группы Эрнеста Мониза, Сэма Нанна и Деса Брауна

В 2013 году Научный комитет Министерства обороны США провел серьезное исследование устойчивости американских оборонных систем к кибератакам. Результаты исследования оказались крайне неутешительными. Совет пришел к выводу, что оборонные системы США страдают от многочисленных уязвимостей, и что правительство США «не готово к отражению этой угрозы».[1]

Авторы исследования, в частности, выразили опасение, что в случае успешной кибератаки военное командование «может утратить доверие к информации, а также уверенность в собственной способность контролировать силы и средства США».[2]

Текст доклада ясно давал понять, что к «силам и средствам» относятся и ядерные вооружения, а также связанные с ними системы управления и связи. *«Военное командование может столкнуться с ложными предупреждениями о нападении либо потерять уверенность в собственной способности контролировать силы и средства США.»* Давайте на минуту задумаемся над этим.

Оказывается, самое смертоносное оружие на планете уязвимо перед лицом невидимых атак со стороны невидимых врагов, причем эти атаки могут привести к самым катастрофическим последствиям.

Сегодня эта проблема актуальна как никогда. Масштабы и природа киберугроз растут и развиваются невиданными темпами – и государственные органы за этими темпами не поспевают. Руководство США и всех остальных ядерных держав просто обязано наверстать отставание, а лучше идти на шаг впереди этих угрозы.

В 2016 году, в рамках усилий по устранению уязвимостей и предотвращению кибератак с потенциально катастрофическими последствиями, NTI опубликовала доклад *«Обуздание киберугрозы: приоритетные задачи в сфере кибер-безопасности ядерных объектов».* В докладе был предпринят анализ следующих возможных сценариев: диверсия против гражданских ядерных объектов, предпринятая террористами или другими хакерскими группами и

1 U.S. Department of Defense, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat* (Washington, DC: Defense Science Board, January 2013), 1, https://www.acq.osd.mil/dsb/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf.

2 Там же, 5

ведущая к выбросу радиации; удаленный захват контроля за ядерным объектом террористами с выдвижением требований; а также использование хакерской атаки для того, чтобы способствовать хищению оружейных ядерных материалов.

В данном докладе под названием «Ядерное оружие в новую кибер-эпоху: Доклад Аналитической группы по изучению киберугроз безопасности ядерных вооружений» предлагается анализ киберугроз безопасности ядерных вооружений, а также рекомендации, разработанные группой бывших и отставных высокопоставленных правительственных чиновников, военных руководителей и экспертов в сфере ядерных систем, ядерной политики и киберугроз.

Пока идёт работа над совершенствованием технических мер безопасности, все ядерные державы также должны найти ответ на несколько стратегических вопросов. Если мы не можем быть до конца уверены в работоспособности наших систем перед лицом атаки со стороны хорошо подготовленного противника, и если у нас нет полной уверенности в нашей способности контролировать собственные ядерные вооружения, то что это означает для дальнейшей актуальности стратегии ядерного сдерживания? Эта стратегия помогла США и СССР пережить Холодную войну, но не стала ли она опасно устаревшей с наступлением эпохи кибер-войн? И не следует ли нам скорректировать нашу ядерную политику и подходы к развертыванию сил, чтобы свести к минимуму потенциальные риски кибератак?

Мы считаем, что США обязаны взять на себя инициативу в сфере борьбы с киберугрозами безопасности любых ядерных объектов и систем – но особенно это относится к безопасности ядерных вооружений. Именно поэтому основное внимание в данном докладе уделяется США. Дальнейшая работа в рамках этого проекта будет направлена на анализ уязвимостей ядерных систем в других государствах, поскольку предотвращение использования ядерного оружия - как террористами, так государствами, как целенаправленного, так и непреднамеренного – является задачей глобального характера. Все страны, обладающие ядерным оружием и ядерными объектами, должны делать больше, много больше, для обеспечения безопасности своих ядерных вооружений и связанных с ними систем. Слабое звено где бы то ни было может привести к глобальной катастрофе.

РЕЗЮМЕ

Основные выводы:

- Успешная кибератака против ядерных вооружений и связанных с ним систем – в т.ч. систем ядерного планирования, раннего предупреждения, оповещения и связи, средств доставки ядерного оружия, а также самого ядерного оружия (объединенных в рамках понятия «системы ядерных вооружений») – может иметь катастрофические последствия.
- Учитывая уровень цифровизации американских систем, а также темпы эволюции киберугроз, нельзя исключить вероятность успешных атак- как в настоящее время, так и в будущем – против любых систем, имеющих цифровые компоненты, в т.ч. систем ядерных вооружений.
- Внедряемые технические меры кибербезопасности имеют огромную важность для защиты от решительно настроенных и хорошо подготовленных противников – однако сами по себе они не могут дать нам достаточной уверенности в безопасности и надежности наших ключевых систем, в т.ч. систем ядерных вооружений.
- Киберугрозы безопасности систем ядерных вооружений увеличивают риск применения этих вооружений в результате ложной тревоги или просчета, а также риск несанкционированного применения ядерного оружия. Такие угрозы могут подорвать уверенность в надежности всей системы ядерного сдерживания, что будет иметь негативные последствия для стратегической стабильности.
- Риск использования ядерного оружия в результате просчета, как и риск несанкционированного применения, существовал и до появления киберугроз, однако такие угрозы усугубляют существующие риски и создают новые. Скорость, скрытность, непредсказуемость и сложность определения источника каждой конкретной кибератаки делают подготовку к таким атакам, их сдерживание и защиту от них очень сложной задачей; гарантированная защита может оказаться попросту невозможной.
- По современным технологическим стандартам многие цифровые ядерные системы давно устарели. В процессе их модернизации нужно проявлять большую осторожность, чтобы не внести в существующие системы новые уязвимости.
- Реагирование на эти угрозы потребует изменений в ядерной политике и стратегии США. Более того, поскольку последствия для стратегической стабильности имеют глобальный характер (и ввиду того, что остальные страны тоже столкнулись с киберугрозой), для решения этой проблемы требуется глобальный подход.

Общие рекомендации

Изложенные в данном докладе рекомендации делятся на четыре нижеприведенных категории. Они представляют первоначальный набор приоритетов общего характера, направленный на минимизацию киберугроз безопасности систем ядерных вооружений и могут послужить отправной точкой для дальнейшего углубленного анализа.

1. *Сокращение риска применения ядерного оружия в результате просчета*
    - Разработка возможных вариантов по увеличению времени принятия решения с учетом киберугроз, стоящих перед системами раннего предупреждения и оповещения.
    - Разработка и внедрение норм, направленных на ограничение использования кибер-оружия против систем ядерных вооружений.
    - Повышение выживаемости и устойчивости ядерных систем и процессов ядерного управления, контроля и связи.

2. *Сокращение рисков для системы ядерного сдерживания*
    - Обеспечение безопасности и диверсификация критически важных систем.
    - Приоритезация мер по сокращению кибер-рисков при разработке планов модернизации.
    - Обеспечение наличия кадрового резерва.

3. *Сокращение риска несанкционированного применения*
    - Укрепление безопасности ядерных вооружений с учетом уязвимости таких вооружений перед лицом гибридных физических/кибер-атак.

4. *Применение глобального подхода к борьбе с киберугрозами безопасности ядерных вооружений*
    - Начало двустороннего диалога с Россией.
    - Укрепление международного сотрудничества по сокращению киберугрозы.

ОСОЗНАНИЕ ПРИРОДЫ КИБЕРУГРОЗ БЕЗОПАСНОСТИ ЯДЕРНЫХ ВООРУЖЕНИЙ И СВЯЗАННЫХ С НИМИ СИСТЕМ

Киберугроза безопасности ядерных вооружений и связанных с ними систем

Киберугрозы актуальны для каждой сферы жизни общества- от финансового сектора до индустрии развлечений, от торговых сетей до страховых компаний. Еще более критический вызов стоит перед правительствами, когда это касается кибератак на критически важные системы. Атаки, направленные на критическую инфраструктуру, могут привести к чрезвычайным последствиям. Однако последствия успешной кибератаки[3] на системы ядерных вооружений – в т.ч. сами ядерные боеголовки, средства их доставки, а также системы ядерного управления, контроля и связи (системы NC3) – могут привести к экзистенциальным последствиям. Кибератаки могут привести к ложным предупреждениям о нападении, парализовать работу критически важных каналов коммуникаций, прервать доступ к информации и поставить под удар системы ядерного планирования и средства доставки ядерных вооружений, или даже позволить злоумышленнику получить контроль над ядерным оружием.

Учитывая уровень цифровизации американских систем, а также скорость эволюции киберугроз, у нас не может быть полной уверенности в том, что имеющие цифровые компоненты системы – в т.ч. системы ядерных вооружений – надежно защищены от нынешних и будущих угроз. Такой вывод основан на нескольких факторах. Ядерные вооружения и средства их доставки периодически подвергаются модернизации, которая может включать в себя установку новых цифровых систем или компонентов. Вредоносный код может быть внедрен в программное обеспечение цифровых систем в процессе их производства, которое зачастую ведется на незащищенных предприятиях. Кроме того, есть зависимость от внешней среды – например, подключения к электросетям – которые напрямую затрагивают ядерные системы, но не контролируются военными. Наконец, всегда существует возможность, что инсайдер – преднамеренно или неумышленно – может способствовать появлению уязвимости кибербезопасности посредством внесения вредоносного кода в одну из критических систем.

3 В данном докладе используется следующее определение кибератаки: под кибератакой понимаются преднамеренные действия с целью нарушить изменить, нарушить, обмануть, ухудшить или уничтожить компьютерные системы, сети, информацию и/или программы, выполняемые в этих системах и сетях либо передаваемые через них. См: National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, ed. William Owens, Kenneth Dam, and Herbert Lin (Washington, DC: National Academies Press, 2009), https://doi.org/10.17226/12651.

Все более широкое использование цифровых систем может также негативно повлиять на выживаемость ядерных вооружений. Новые технологии могут повысить надежность и эффективность – но при этом они также могут привести к появлению новых уязвимостей в некогда высокоустойчивых системах, например, в подводных лодках или мобильных пусковых установках.[4]

В Обзоре ядерной политики США, опубликованной администрацией Дональда Трампа, признается наличие киберугроз безопасности ядерных систем управления, контроля и связи (системы NC3): «Появление наступательного кибер-оружия создает вызовы и потенциальные уязвимости в системах NC3. Потенциальные противники прилагают значительные усилия к разработке и применению кибер-оружия против сетевых систем. Хотя на сегодняшний день наши системы NC3 надежно защищены и эффективны, мы предпринимаем меры реагирования на вызовы в сфере сетевой защиты, проверок подлинности, целостности данных и обеспечения безопасного, гарантированного и надежного потока информации в устойчивых сетях NC3.»[5]

ВНЕДРЯЕМЫЕ ТЕХНИЧЕСКИЕ МЕРЫ КИБЕРБЕЗОПАСНОСТИ ИМЕЮТ ОГРОМНУЮ ВАЖНОСТЬ – НО САМИ ПО СЕБЕ ОНИ НЕ ДАЮТ НАМ ДОСТАТОЧНОЙ УВЕРЕННОСТИ В БЕЗОПАСНОСТИ И НАДЕЖНОСТИ НАШИХ КЛЮЧЕВЫХ СИСТЕМ, В Т.Ч. СИСТЕМ ЯДЕРНЫХ ВООРУЖЕНИЙ.]

Это признание следует за более ранними исследованиями, в которых признавался подлинный масштаб киберугроз безопасности систем ядерных вооружений и звучали предупреждения относительно невозможности эффективного реагирования на такие угрозы одними лишь техническими средствами. В 2013 году Научный комитет Министерства обороны США провел серьезное исследование и сформулировал рекомендации по укреплению устойчивости систем министерства обороны к кибератакам. В своем докладе Комитет, в частности, пришел к следующему тревожному выводу: «У США нет полной уверенности в том, что наши критические IT-системы сохранят работоспособность в условиях атаки со стороны хорошо подготовленного и обладающего значительными ресурсами противника».[6] Комитет также заключил, что ни один из существующих технических подходов не способен обеспечить «полную» защиту министерства обороны от решительно настроенного противника. В докладе Совета содержится рекомендация «немедленно предпринять меры для оценки выживаемости нынешнего поколения американских средств ядерного сдерживания и предоставления соответствующих заверений руководству США»[7] с учетом наиболее значимых киберугроз, определенных в докладе.

Во втором докладе, опубликованном Научным комитетом Министерства обороны США в январе 2017 года, Пентагону рекомендуется предпринять ряд инициатив,

4 Paul Bracken, "The Intersection of Cyber and Nuclear War," *Real Clear Defense*, January 17, 2017, https://www.realcleardefense.com/articles/2017/01/17/the_intersection_of_cyber_and_nuclear_war_110646.html.
5 U.S. Department of Defense, Office of the Secretary of Defense, *Nuclear Posture Review* (Washington, DC: Department of Defense, February 2018), 57, https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF
6 U.S. Department of Defense, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat* (Washington, DC: Defense Science Board, January 2013), 1, https://www.acq.osd.mil/dsb/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf.
7 Defense Science Board (2013), 42

включая планирование и проведение кампаний направленного сдерживания, создание устойчивой к кибер-атакам сети коммуникаций ключевых американских ядерных и неядерных ударных систем, а также укрепление устойчивости США перед лицом кибератак, в т.ч. путем наращивания возможностей по определению источника кибератак.[8]

Доклады Научного комитета Министерства обороны США и последующие дискуссий с экспертами привели NTI к выводу о том, что киберугроза носит такой характер, который *в качестве наивысшего приоритета требует особых мер по защите систем ядерных вооружений.* Эксперты NTI также полагают, что *хотя внедряемые технические меры кибербезопасности имеют огромную важность, сами по себе они не могут дать нам достаточной уверенности в безопасности и надежности наших ключевых систем, в т.ч. систем ядерных вооружений.*

Хотя нынешняя администрация в недавно выпущенном Обзоре ядерной политики США заверяет, что «системы NC3 надежно защищены и эффективны», такая оценка в лучшем случае может отражать ситуацию лишь на момент публикации этого документа. Мы полагаем, что более реалистичная оценка киберугрозы дана на страницах доклада Научного комитета Министерства обороны США, вышедшего в 2013 году. Выводы этого доклада о том, что правительство больше не в состоянии гарантировать – ни в настоящее время, ни в будущем – что системы ядерных вооружений всегда будут функционировать должным образом (или что их можно полностью обезопасить от несанкционированного применения), вкупе с неизбежным предположением о том, что все остальные ядерные державы наверняка столкнулись с аналогичной проблемой, имеют значительные последствия. На сегодня не осталось сомнений, что киберугрозы безопасности систем ядерных вооружений увеличивают риск применения ядерного оружия в результате просчета, риск несанкционированного применения, а для некоторых способны подорвать уверенность в ядерном сдерживании, оказывая таким образом негативное влияние на стратегическую стабильность. Решение этих проблем потребует корректировки ядерной политики и стратегии США – как и, по всей вероятности, всех остальных ядерных держав.

Насколько реальна угроза?

На данный момент не сообщалось о реальных случаях кибератак, направленных против систем ядерных вооружений – однако исторические параллели демонстрируют масштаб возможных последствий таких атак. К примеру, в 1980 году американские системы раннего предупреждения о ракетном нападении выдали сигнал, что по США выпущены ракеты.[9] За минуты до отдачи президентом США приказа о нанесении ответного удара выяснилось, что предупреждение было ложной тревогой, и что ее причиной стал сбой в компьютерном чипе. А всего несколько лет назад, в 2010 году, 50 развернутых в Вайоминге ядерных ракет оказались в нерабочем состоянии из-за аппаратного сбоя в компьютерном оборудовании; на устранение поломки ушел почти час.[10]

8 U.S. Department of Defense, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Defense Science Board, *Task Force on Cyber Deterrence* (Washington, DC: Defense Science Board, February 2017), https://www.acq.osd.mil/dsb/reports/2010s/DSB-cyberDeterrenceReport_02-28-17_Final.pdf.

9 Patricia M. Lewis, Heather Williams, Benoît Pelopidas, and Sasan Aghlani, *Too Close for Comfort: Cases of Near Nuclear Use and Options for Policy* (London: Chatham House, 2014), https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20140428TooCloseforComfortNuclearUseLewisWilliamsPelopidasAghlani.pdf

10 "Air Force Loses Contact with 50 ICBMs at Wyoming Base," Nuclear Threat Initiative, October 27, 2010, http://www.nti.org/gsn/article/air-force-loses-contact-with-50-icbms-at-wyoming-base/.

> **"Крайне важно регулярно проводить анализ кибер-уязвимостей нашего ядерного арсенала и устранять все выявленные проблемы, поскольку наши противники наверняка заняты поиском этих уязвимостей. Мы обязаны найти и устранить эти уязвимости первыми."**
>
> *—Дебора Планкет*
> ЧЛЕН ГРУППЫ]

Подобные инциденты – особенно если они случатся во время кризиса или конфликта – могут поставить руководство страны на грань отдачи приказа о ядерном ударе по противнику на основании недостоверной информации. Они также могут подорвать уверенность в надежности военных систем, а без этой уверенности вероятность непоправимых ошибок многократно возрастает.

Киберугрозы быстро эволюционируют, однако на сегодняшний день наибольшую обеспокоенность в плане кибератак против систем ядерных вооружений вызывают следующие риски.

- **Риск применения ядерного оружия в результате просчета.** С учетом сегодняшней ядерной стратегии- около 1000 ракет с ядерными боеголовками, готовых к запуску в течение минут, и наземные силы, уязвимые для обезоруживающего первого удара – кибератака на систему раннего предупреждения, достоверно имитирующая ядерную атаку, создает риск ядерного ответа в результате просчета. Аналогичным образом, в ходе конфликта риск подобного удара в результате просчета также возрастает в случае обнаружения вредоносного кода в программном обеспечении систем управления ядерными вооружениями, потенциально способного вывести из строя американские стратегические средства либо какой-либо из их компонентов. В случае нанесения противником первого удара понадобится быстро запустить американские межконтинентальные баллистические ракеты (МБР), чтобы они не оказались уничтоженными на земле. В частности, в силу этой причины у президента США будет очень мало времени на принятие решения о том, отдавать ли приказ на запуск МБР на основании имеющейся информации о первом ударе противника (которая может оказаться ложной тревогой, вызванной кибер средствами или другим способом).
- **Риск несанкционированного применения.** Кибератаки могут использоваться в сочетании с физическими атаками для обхода мер обеспечения безопасности ядерных вооружений, с целью хищения либо несанкционированного применения ядерного оружия, что может привести к катастрофическим последствиям. Еще один возможный, хотя и менее вероятный сценарий – это незаконный или несанкционированный приказ о применении ядерного оружия, отданный злоумышленником через взломанную систему управления.
- **Снижение уверенности в эффективности ядерного сдерживания и негативное влияние на стратегическую стабильность.** Помимо увеличения риска несанкционированного применения ядерного оружия или применения в результате просчета, киберугрозы безопасности ядерных вооружений ставят под удар основы ядерного сдерживания, подрывая таким образом

стратегическую стабильность. С точки зрения ядерного сдерживания и стратегической стабильности та неопределенность, которая вытекает из уникальной природы киберугроз, представляет собой опасность иного характера, чем новые разработки в сфере ядерных и неядерных вооружений. К примеру, кибератаки против систем связи могут нарушить обмен информацией, жизненно необходимой для принятия решений о применении ядерного оружия, в т.ч. для реагирования на предупреждение о нападении противника. Такие кибератаки могут прервать цепочку передачи приказа о применении ядерного оружия; нарушить работу международных каналов связи, необходимых для де-эскалации кризиса; либо привести к неправильной трактовке происходящего в случае атаки на системы двойного назначения, когда нет возможности прояснить намерения атакующей стороны. Кроме того, преднамеренное внесение ошибок или вредоносного кода в программное обеспечение ядерных вооружений через цепочку поставок на этапе их производства, ведущее к ухудшению их рабочих характеристик, может подорвать уверенность в ядерном сдерживании. Уверенность руководства страны в том, что все ее ядерные системы сработают должным образом (как и аналогичная уверенность в этом со стороны противника) является ключевым компонентом всей концепции ядерного сдерживания. Потеря уверенности в собственной способности предотвратить ядерную атаку противника инструментами ядерного сдерживания будет иметь серьезные негативные последствия для стратегической стабильности.

Подготовка к запуску спутника системы космического наблюдения, 2008 г.]

Следует подчеркнуть, что все эти риски существовали и до появления новых киберугроз. За почти 70 лет существования на планете ядерного оружия неоднократно случались ложные тревоги из-за человеческого фактора или технических сбоев. Однако киберугроза усугубляет эти риски и создает новые. Скорость, скрытность, непредсказуемость и сложность определения источника каждой конкретной кибератаки делают подготовку к таким атакам, равно как и сдерживание и защиту от них, очень сложной, если не невозможной, задачей. Кроме того, системы ядерных вооружений используют в своей работе множество цифровых компонентов, в т.ч. связанных с гражданскими системами.

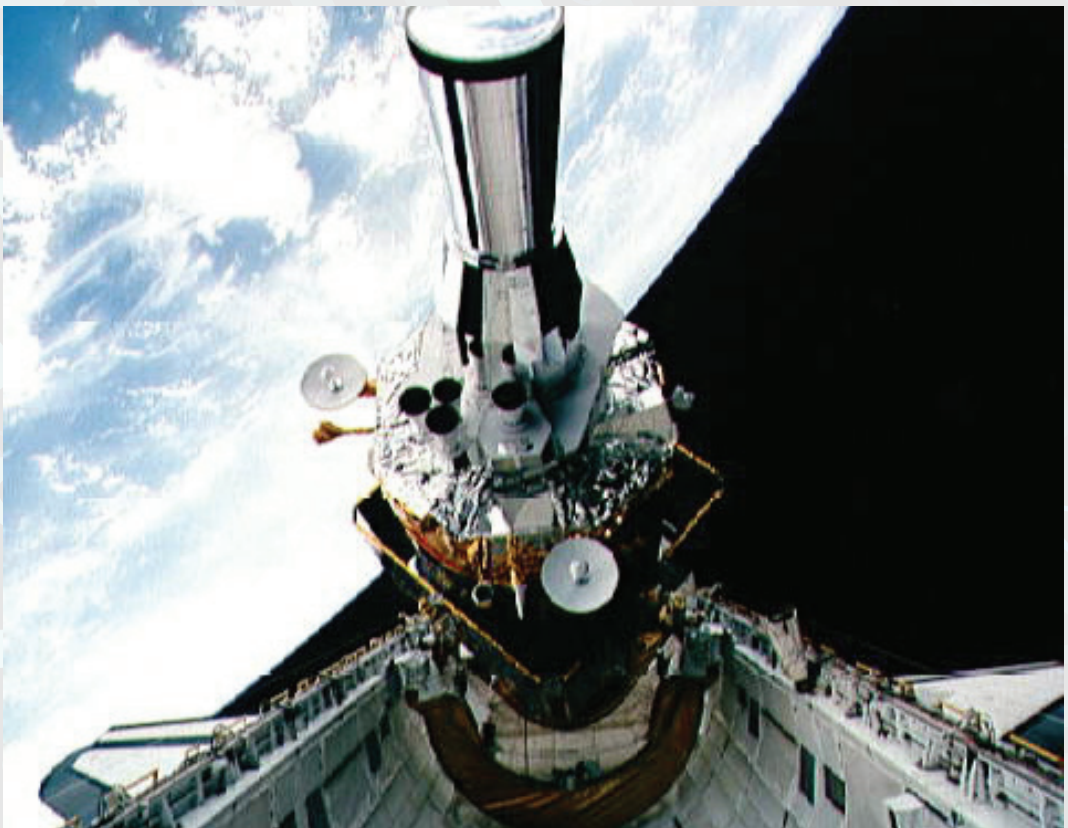
В силу уникального характера и последствий кибер-рисков, рекомендации по их сокращению должны быть выполнены самым неотложным образом, особенно учитывая, что США в настоящее время внедряют меры, перечисленные в Обзоре ядерной политики США, опубликованном администрацией Трампа. Этот документ определяет приоритеты, затрагивающие политику применения ядерного оружия, стратегию ядерных сил, их структуру и планы по их модернизации на следующие несколько лет.

СИСТЕМЫ ДВОЙНОГО НАЗНАЧЕНИЯ И ПРОБЛЕМА СОКРАЩЕНИЯ РИСКОВ

Многие системы управления, контроля и связи (системы С3) являются системами двойного назначения. Примером таких систем являются спутники, использующиеся как в неядерных, так и в ядерных целях. Это создает дополнительные риски в случае кибератак. Атаки на системы С3, которые зачастую предпринимаются на ранних этапах неядерных конфликтов, могут быть истолкованы жертвой такой атаки как попытка лишить страну способности применить свой ядерный арсенал.

Интеграция неядерных и ядерных С3-систем имеет множество причин. В некоторых случаях она обусловлена стремлением уменьшить количество одновременно используемых систем или сократить расходы. В иных случаях это может делаться сознательно с целью сдерживания возможных атак на такие системы. Однако в любом случае атака на системы С3 – как осознанная, так и непреднамеренная – будет воспринята в качестве попытки нарушить работу системы ядерного сдерживания.

Чтобы сократить этот риск, США и другие ядерные державы могли бы взять на себя обязательство не атаковать С3-системы, связанные с ядерным оружием. Однако с учетом высокой степени интеграции многих подобных систем достижение подобного соглашения может оказаться сложным. Даже если соглашение все-таки будет заключено, верифицировать его соблюдение будет практически невозможно. В качестве альтернативы государства могли бы договориться о четком разделении своих ядерных и неядерных систем, а также заявить о том, что любая атака на ядерную систему будет иметь серьезные последствия. Подобное соглашение может оказаться полезным с течением времени, однако для его выполнения понадобятся постоянные усилия, направленные на недопущение любой непреднамеренной интеграции между ядерными и неядерными системами.



Спутник системы предупреждения о ракетном нападении, выведенный на орбиту космическим челноком «Спейс шаттл» в ходе миссии STS-44 в 1991 году]

> **“Киберугроза безопасности ядерных вооружений является международной проблемой; ее решение потребует тесного международного сотрудничества. Все страны мира глубоко заинтересованы в предотвращении кибератак, способных привести к ядерному взрыву либо спровоцировать, обострить и углубить ядерный кризис. Поэтому наиболее актуальная задача на сегодня — это усадить все ядерные державы за стол переговоров в поисках соглашения о предотвращении наиболее опасных сценариев, к которым может привести новая киберугроза.”**
>
> *—Эндрю Фаттер*
> ЧЛЕН АНАЛИТИЧЕСКОЙ ГРУППЫ]

Четыре показательных сценария

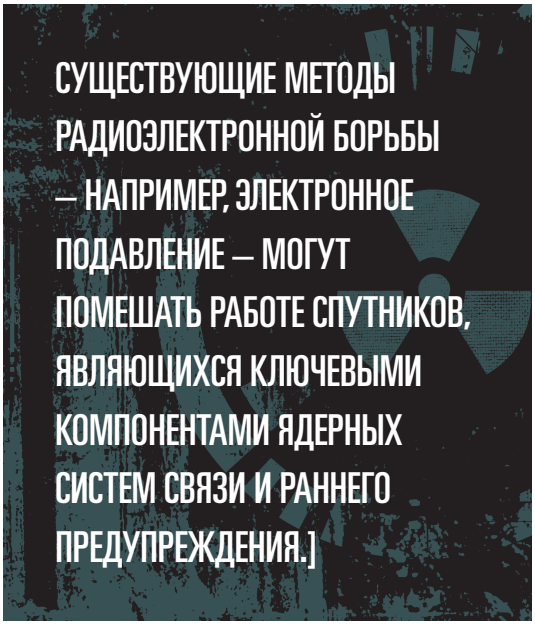
Аналитическая группа рассмотрела четыре сценария, демонстрирующих возможные последствия киберугроз безопасности ядерных вооружений и связанных с ними систем. В ходе анализа этих сценариев Группа не ограничивалась последствиями кибератак на системы ядерных вооружений (т.е. вероятностью несанкционированного применения ядерного оружия или же его применения в результате просчета). Члены Группы также обсуждали вопрос о том, как эти уязвимости и риски влияют на стратегическую стабильность и ядерное сдерживание, подрывая уверенность в системе ядерного сдерживания. Группа пришла к выводу, что киберугрозы потенциально могут серьезно подорвать доверие к системам ядерных вооружений.

Рассмотренные Группой сценарии представляются вполне реалистичными; они отражают наиболее значительные угрозы и уязвимости, имеющиеся в системах ядерных вооружений. Минимизация этих угроз и уязвимостей имела бы серьезные положительные последствия для защиты систем ядерных вооружений от кибератак и предотвращения других, менее катастрофичных сценариев. Вероятность попыток осуществления какого-либо из описанных сценариев государственными или негосударственными игроками зависит от конкретной ситуации и будет постоянно меняться с течением времени. Кроме того, любой анализ должен учитывать роль, которую могут сыграть инсайдеры (как преднамеренно, так и без злого умысла).

Сценарий № 1: В разгар кризиса системы раннего предупреждения выдают ложную тревогу о ядерном нападении

В момент, когда напряженность в отношениях с Россией достигла наивысшей точки со времен окончания Холодной войны, компьютеры Командования воздушно-космической обороны Североамериканского континента (NORAD) выдают предупреждение, что по США запущено множество баллистических ракет. Дело происходит глубокой ночью, и когда Белому дому сообщают, что по США, возможно, вот-вот будет нанесен катастрофический ядерный удар, у президента и его военных советников есть всего несколько минут, чтобы принять решение о том,

как реагировать. Президент и его советники осознают возможность того, что наша система предупреждения о ядерном нападении выдала ложную тревогу, но у них слишком мало времени, чтобы достоверно это установить. Нужно срочно принимать решение о запуске американских ракет и нанесении ответного удара, иначе значительная часть американских ядерных вооружений может быть уничтожена в ходе первого удара.[11]



Насколько реален такой сценарий?

Этот сценарий совершенно реален. Хотя системы раннего предупреждения хорошо защищены, на реальность подобного сценария указывают как минимум два инцидента. В 1980 году аппаратный сбой в одном из компьютеров NORAD привел к выдаче ложного сигнала тревоги о запуске по США ядерных ракет[12], а в 1983 году советские военные приняли отражение солнечных лучей от облаков за пять летящих ракет.[13] Эти инциденты были вызваны человеческой либо технической ошибкой, а не чьими-то злонамеренными действиями – но аналогичные инциденты могут быть спровоцированы и преднамеренно. К примеру, на определенном этапе производства ракетных компонентов можно внести несанкционированные изменения в инфракрасные датчики, которые обнаруживают реактивную струю летящих ракет. Или же, можно также внедрить ложный сигнал о ракетной атаке в компьютеры системы раннего предупреждения.[14]

Инициаторами такого сценария с наибольшей вероятностью могут стать негосударственные игроки или третья сторона.

Сценарий № 2: Кибератака нарушает работу систем, обеспечивающих связь между государственным руководством, операторами ядерных систем и самими системами и/или иностранными партнерами в разгар потенциального кризиса

В разгар политического кризиса между Россией и США российское военное командование безуспешно пытается связаться с американскими коллегами, чтобы определить достоверность полученного сигнала о ракетном нападении (который, как они подозревают, является результатом хакерской атаки). Российские военные знают, что в течение последних нескольких месяцев хакеры пытались проникнуть в их компьютерные системы, но не имеют возможности с точностью определить, является ли сигнал о ракетном нападении подлинным или нет. Системы связи, которые им нужны для де-эскалации кризиса, не работают.

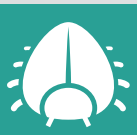
11 Есть и альтернативный сценарий, который более вероятен, если противником является государственный игрок: целью кибератаки может быть нарушение работы системы раннего предупреждения, чтобы она не среагировала на ядерную атаку.

12 "The 3 A.M. Phone Call," The Nuclear Vault, *The National Security Archive*, March 1, 2012, https://nsarchive.gwu.edu/nukevault/ebb371/.

13 Anthony M. Barrett, "False Alarms, True Dangers? Current and Future Risks of Inadvertent U.S.-Russian Nuclear War," (Santa Monica, CA: Rand Corporation, 2016), https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE191/RAND_PE191.pdf.

14 Lee Billings, "War in Space May Be Closer Than Ever," *Scientific American*, August 10, 2015, https://www.scientificamerican.com/article/war-in-space-may-be-closer-than-ever/; Colin Clark, US Challengers Can Spoof, Dazzle, Cyber Attack US Satellites: DepSecDef, *Breaking Defense*, April 13, 2016, https://breakingdefense.com/2016/04/us-challengers-can-spoof-dazzle-cyber-attack-us-satellites-depsecdef/; Patricia Lewis and David Livingstone, "The Cyber Threat in Outer Space," *Bulletin of the Atomic Scientists,* November 21, 2016, https://thebulletin.org/cyber-threat-outer-space10178

ОСНОВНЫЕ КИБЕР-УЯЗВИМОСТИ И ПОТЕНЦИАЛЬНЫЕ ПОСЛЕДСТВИЯ

	ТОЧКА УЯЗВИМОСТИ	ТИП АТАКИ	ПОТЕНЦИАЛЬНЫЕ ПОСЛЕДСТВИЯ
	Системы раннего предупреждения: радары и спутники	Внедрение ложной информации о ядерном нападении	«Ответный» ядерный удар, спровоцированный ложным предупреждением
	Системы коммуникаций	Кибератака приводит к отказу каналов связи между официальными лицами, операторами/системами и иностранными партнерами	Ядерный удар, нанесенный на основании неправильно истолкованной информации или из-за невозможности де-эскалации ЛИБО Потеря уверенности в том, что приказ о нанесении ответного удара в ответ на ядерное нападение будет выполнен
	Производственная цепь	Внедрение вредоносного кода в один из компонентов ядерного оружия на этапе производства	Потеря уверенности в том, что ядерное оружие будет функционировать должным образом as intended
	Системы безопасности	Кибератака приводит к отказу или неэффективности систем безопасности/физической защиты	Хищение ядерного оружия

Этот сценарий, основанный на неработоспособности ключевых систем связи в разгар ядерного кризиса, имеет несколько вариантов. Может быть нарушена работа каналов связи между членами руководства страны; между операторами ядерных систем и самими системами; либо между военно-политическим руководством страны и иностранными партнерами. Противник также может прибегнуть к кибератаке в следующих целях:

- Нарушить или полностью прервать связь между политическим руководством страны и военными, либо парализовать работу каналов, по которым передается приказ о применении ядерного оружия, делая таким образом невозможным принятие информированных решений о реагировании на ядерную атаку или отдачу приказа о нанесении ответного удара.
- Нарушить или полностью прервать связь между операторами ядерных систем и самими системами, лишая операторов возможности получить от этих систем данные, необходимые руководству, либо передать данные на эти системы.

- Нарушить работу каналов связи двойного назначения (ядерных и неядерных) в рамках стратегии по подрыву неядерного военного потенциала США на ранних этапах конфликта;
- Нарушить или прервать связь между военно-политическим руководством разных стран, чтобы не дать им возможности предпринять усилия по де-эскалации.

Насколько реален такой сценарий?

На реальность этого сценария указывают несколько инцидентов. В 2010 году технический сбой привел к 45-минутному отсутствию связи с 50 МБР с ядерными боеголовками, развернутыми в Вайоминге.[15] Аналогичного результата можно было бы добиться и с помощью кибератаки. Многочисленные примеры хакерских атак типа DDoS демонстрируют, что нарушение работы ключевых узлов коммуникационной инфраструктуры может полностью парализовать связь между пользователями. В 2015 году DDoS-атака на украинские электросети нарушила работу телефонов абонентского центра компании-оператора, не давая таким образом потребителям сообщить, что они остались без электричества.[16] Еще одна атака была предпринята с помощь червя Slammer, который перегружает сеть и ведет к отказу серверов баз данных, забивая все каналы связи собственным трафиком.[17] Этим червем в 2003 году оказались заражены компьютеры АЭС Дэвис-Бесс в штате Огайо. В результате на станции целых 5 часов на экраны не выводилась информация о состоянии основных систем безопасности и активной зоны реактора. Подобные технологии теоретически можно использовать для того, чтобы оставить без связи системы управления ядерным оружием, в результате чего их использование окажется невозможным в самый разгар кризиса. Кроме того, давно отработанные меры радиоэлектронной борьбы – например, системы электронного подавления – могут быть использованы против спутников, являющихся ключевым компонентом ядерных систем коммуникаций и раннего предупреждения.[18]

Сценарий № 3: Противник внедряет дефект или вредоносный код в ядерное оружие на этапе производства его компонентов или другим способом, потенциально подрывая эффективность затронутых систем вооружений.

В процессе производства и сборки цифровых компонентов ядерного оружия или средств их доставки противник может скрытно, используя пробелы в системе проверок поставщиков на благонадежность и безопасность, внедрить вредоносный код в один из компонентов. Этот код затем можно будет активировать в любое время (в т.ч. в разгар кризиса), подорвав тем самым уверенность в надежности ядерных вооружений, нарушив их работу и спровоцировав дальнейшую эскалацию

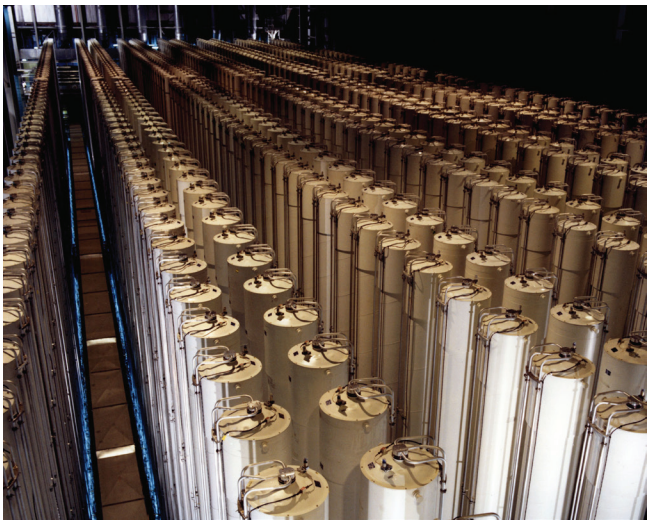
15 Bruce Blair, "Could Terrorists Launch America's Nuclear Missiles?" *Time*, November 11, 2010, http://content.time.com/time/nation/article/0,8599,2030685,00.html.

16 Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

17 David Moore, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford, and Nicholas Weaver, "Inside the Slammer Worm," *Security & Privacy Magazine,* IEEE Computer Society, July/August 2003, http://www.icsi.berkeley.edu/pubs/networking/insidetheslammerworm03.pdf.

18 Robert K. Ackerman, "Space Vulnerabilities Threaten U.S. Edge in Battle," *Signal*, AFCEA, June 2005, http://www.afcea.org/content/?q=space-vulnerabilities-threaten-us-edge-battle; FAS Panel on Weapons in Space, "United States Space Systems: Vulnerabilities and Threats," in En*suring America's Space Security: Report of the FAS Panel on Weapons in Space* (Washington, DC: Federation of American Scientists, September 2004), https://fas.org/pubs/_docs/10072004163734.pdf

кризиса. Более того, к тем же самым последствиям могут привести даже ложные, но внушающие доверие, заявления о внедрении вредоносного кода в системы ядерных вооружений.



Каскад газовых центрифуг на американском заводе по обогащению урана]

Более вероятным (и более опасным) сценарием может стать обнаружение дефекта или вредоносного кода до того, как этот дефект или код будут использованы противником. Это может привести к дальнейшей дестабилизации в разгар кризиса, когда сохраняется неясность относительно намерений противника. Это в особенности применимо к случаям внедрения кода в системы двойного назначения (ядерным и неядерным) – например, в американские спутники системы раннего предупреждения иуправления и связи. Военно-политическому руководству в такой ситуации придется решать, как реагировать и реагировать ли вообще; является ли проблема изолированной или масштабной; насколько велика вероятность обнаружения дальнейших дефектов или других видов вредоносного кода; и насколько велик риск реальной атаки с использованием этих дефектов. При наиболее экстремальном (но и наименее вероятном) сценарии сообщения о найденных в американском ядерном оружии дефектах могут спровоцировать противника на нанесение первого удара или вынудить США по причине отсутствия уверенности в эффективности собственных ядерных вооружений применить оружие во избежание риска его потери.

Насколько реален такой сценарий?

Обеспокоенность по поводу внедрения дефектов или вредоносного кода на этапе производства высказывалась и применительно к другим областям. Исследовательский департамент ВВС США в 2016 году изучал этот вопрос применительно к поставкам собственных электронных компонентов. В ходе семинара несколько докладчиков, представляющих промышленность, подтвердили, что риск компрометации оборонной производственной цепи вполне реален, и что существует серьезная озабоченность по поводу возможности внедрения вредоносного кода в электронные компоненты на этапе производства и сборки.[19]

Хотя многие ключевые компоненты ядерного оружия производятся на специальных объектах с особыми мерами безопасности, нельзя с уверенностью сказать, что все без исключения компоненты, используемые в системах управления и связи, надежно защищены от попыток внедрения вредоносного кода. Как утверждает Национальная администрация США по вопросам ядерной безопасности, «Тенденция к приобретению компонентов ядерных вооружений у иностранных поставщиков может нести в себе риск для безопасности этих вооружений.»[20] В силу огромной сложности современных ядерных вооружений уязвимости существуют на многих этапах их производства.

19 Optimizing the Air Force Acquisition Strategy of Secure and Reliable Electronic Components: Proceedings of a Workshop (Washington, DC: National Academies Press, 2016), http://www.nap.edu/read/23561/chapter/2

20 "DOE Should Assess Circumstances for Using Enhanced Procurement Authority to Manage Risk," GAO Highlights, August 2016, http://www.gao.gov/assets/680/678999.pdf.

"Системы ядерных вооружений, вероятно, будут оставаться уязвимыми для киберугроз несмотря на укрепление мер кибер-безопасности в будущем. В этой связи необходимо внести коррективы в ядерную стратегию, чтобы компенсировать связанные с киберугрозой риски."

—Херб Лин
ЧЛЕН АНАЛИТИЧЕСКОЙ ГРУППЫ]

Противник также может внедрить «спящий» вредоносный код в одну из критических систем, чтобы затем активировать его в ходе конфликта. Судя по сообщениям, появившимся в 2017 году, администрация Обамы разрабатывала планы тайного внедрения кибер-оружия в элементы критической российской инфраструктуры.[21] В начале 2018 года официальные лица США заявляли, что российским хакерам удалось создать плацдарм в критической инфраструктуре США и Европы.[22] Хотя неясно, насколько эта программа продвинулась вперед, эти сообщения свидетельствуют об интересе к созданию латентного кибер-потенциала, который можно было бы использовать в будущем. Сообщалось также, что США и другие государства – такие как РФ и Китай – уже используют разнообразные наступательные кибер-средства в поддержку своих военных операций, в т.ч. антитеррористических.[23]

Наконец, пока неясно, в какой степени критические системы, связанные с ядерным оружием, можно изолировать от неядерных систем, поэтому противник может неправильно оценить риски и альтернативы, связанные с попытками атаковать системы двойного (ядерного/неядерного) назначения.

21 Greg Miller, Ellen Nakashima, and Adam Entous, "Obama's Secret Struggle to Punish Russia for Putin's Election Assault," Washington Post, June 23, 2017, https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/.

22 См. например: Nicole Perlroth and David E. Sanger, "Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says," New York Times, March 15, 2018, https://www.nytimes.com/2018/03/15/us/politics/russia-cyberattacks.html.

23 David E. Sanger, "U.S. Cyberattacks Target ISIS in a New Line of Combat," New York Times, April 24, 2016, https://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html

Сценарий 4: Противнику удается получить несанкционированный контроль над ядерным устройством путем его хищения и/или обхода систем безопасности с использованием кибер-инструментов.

В разгар серьезного политического кризиса и протестов в одной из европейских стран, где находится американское ядерное оружие передового базирования, командование военной базы на какое-то время утратило контроль над объектами хранения ядерного оружия, поскольку была нарушена работа систем безопасности базы. Через несколько недель оказывается, что с базы пропала как минимум одна ядерная боеголовка.

Насколько реален такой сценарий?

Данный сценарий включает в себя хищение или другой способ получения несанкционированного контроля над ядерным оружием либо одним из его компонентов, потенциально ведущие к несанкционированному применению. Вероятность внедрения ложной команды на применение ядерного оружия путем «взлома» системы управления является менее высокой по сравнению с другими сценариями, однако в будущем этот риск может возрасти.

Случаи сбоев в системах управления и безопасности ядерного оружия передового базирования в прошлом, а также установленные случаи использования кибер-средств для взлома систем контроля доступапредполагают, что рассматриваемый сценарий также должен являться предметом озабоченности.

В 2016 году американское ядерное оружие, развернутое на военно-воздушной базе Инджирлик в Турции в рамках натовской программы расширенного сдерживания, оказалось под серьезной угрозой из-за попытки военного переворота. Подача электроэнергии на базу была отключена, всем самолетам ВВС США в Турции было приказано оставаться на земле, а турецкий командующий базой был задержан по подозрению в участии в путче. Подобные хаотические ситуации нельзя исключить и в будущем; особенно это относится к оружию передового базирования. Противник может попытаться воспользоваться кибер-средствами для взлома систем защиты ядерных систем от несанкционированного доступа.

ТЕКУЩИЕ МЕРЫ, ПРЕДПРИНИМАЕМЫЕ США ДЛЯ БОРЬБЫ С КИБЕРУГРОЗАМИ БЕЗОПАСНОСТИ ЯДЕРНЫХ ВООРУЖЕНИЙ

На основании опубликованной информации можно сделать вывод, что США уделяют все больше внимания киберугрозам безопасности ядерных вооружений. Хотя конкретные подробности соответствующих программ не публикуются, определенные выводы об их приоритетах в области повышения киберустойчивости можно сделать на основании данных об оборонном бюджете США.

К примеру, и ВМФ, и ВВС США выделили около 500 миллионов долларов на модернизацию стратегических систем управления. В рамках этой модернизации проводится усовершенствование всех звеньев системы коммуникаций между составными элементами ядерной триады и Национальным командованием. Укрепление мер кибербезопасности указано в качестве одного из приоритетов модернизации по нескольким индивидуальным программам. Кроме того, в своей бюджетной заявке Конгрессу на 2018 финансовый год Национальное управление ядерной безопасности (NNSA) запросило более 186 миллионов долларов из оружейного бюджета на усовершенствование своих информационных систем и дополнительные меры кибербезопасности. Часть этих средств может быть потрачена на усилия по минимизации кибер-уязвимостей в ядерных вооружениях, но она не может быть напрямую связана с этими усилиями.

Еще одно свидетельство того, что укрепление кибербезопасности систем управления и связи рассматривается в качестве ключевого приоритета, содержится в Законе о расходах на национальную оборону в 2018 году, вступившем в силу 12 декабря 2017 г. В Пункте 1651 этого Закона командующим Стратегического командования США и Кибер-командования США поручено проводить ежегодную совместную оценку устойчивости систем ядерного управления к киберугрозам. Кроме того, в Пункте 1640 министру обороны США поручено разработать совместно с директором Управления национальной безопасности план создания «Стратегической программы кибербезопасности» Министерства обороны США. В задачи этой программы входят меры по укреплению кибербезопасности различных систем, в том числе: (а) наступательных кибер-систем, (б) ударных систем большой дальности, (в) систем ядерного сдерживания, (г) систем национальной безопасности, и (д) критической инфраструктуры Министерства обороны. Аналогичные рекомендации содержались и в докладе, опубликованном в 2017 году Научным советом Пентагона – где, в частности, говорилось о необходимости создания сети кибер-устойчивых систем практически в тех же самых категориях.

Эти и другие усилия призваны сыграть важную роль в сокращении риска кибератак против систем ядерных вооружений. Однако, как уже говорилось в данном докладе, при всей важности технических мер, ни одно технологическое решение само по себе не может быть абсолютно эффективным. Необходимо также вносить изменения в ядерную политику и стратегию.

ОБЩИЕ РЕКОМЕНДАЦИИ

Руководящие принципы

На основании вышеуказанных четырех сценариев, послуживших основой для дискуссий и обсуждений, эксперты NTI при участии Аналитической группы разработали рекомендации по сокращению риска кибератак против ядерных вооружений, способных привести к катастрофическим последствиям. Рекомендации были разработаны на основе следующих руководящих принципов:

1. **Пока ядерное оружие остается центральным элементом стратегии безопасности США, у Соединенных Штатов будет сохраняться потребность в надежных и безопасных средствах ядерного сдерживания.**

   Пока ядерное оружие продолжает играть важную роль в стратегии сдерживания, необходимо предпринимать меры по максимально возможному сокращению киберугроз ядерным вооружениям, даже если добиться полного устранения всех рисков не удастся. Эволюция киберугроз будет идти настолько быстрыми темпами, что для минимизации рисков для безопасности ядерных вооружений понадобится вносить серьезные изменения в стратегию, политику и структуру систем ядерных вооружений.

2. **Полностью устранить киберугрозу безопасности ядерных вооружений одними лишь техническими мерами не удастся.**

   Хотя технические меры кибербезопасности будут иметь огромную важность и должны развиваться, самих по себе этих мер будет недостаточно для гарантирования безопасности и надежности критических систем, в т.ч. ядерного оружия. Наоборот, руководство США должно исходить из предположения, что с учетом нынешнего уровня проникновения цифровых технологий и темпов эволюции киберугроз, все системы, имеющие цифровые компоненты – в т.ч. ядерное оружие – уже могут быть скомпрометированы.[24]

3. **Киберугроза является глобальным вызовом и одностороннего подхода в этой сфере будет недостаточно.**

   Киберугроза стоит перед всеми ядерными державами, поэтому здесь необходимы двусторонние и многосторонние меры. Хотя в данном докладе основное внимание уделяется угрозами и уязвимостям, актуальным для США, а большинство приведенных рекомендаций предназначено для американского руководства, одних лишь односторонних мер, предпринимаемых Соединенными Штатами, будет недостаточно. Более того, в некоторых случаях односторонние шаги могут лишь усугубить нестабильность, особенно если усилия США по укреплению безопасности собственных систем приведут к значительной асимметрии между разными странами в плане безопасной и гарантированной работы своих систем.

24 Richard Danzig, "Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies," Center for a New American Security, July 21, 2014, https://www.cnas.org/publications/reports/surviving-on-a-diet-of-poisoned- fruit-reducing-the-national-security-risks-of-americas-cyber-dependencies

Рекомендации

В рекомендациях, приведенных в данном разделе, перечислены приоритетные меры по минимизации киберугрозы безопасности ядерных вооружений. Некоторые из этих мер в той или иной степени уже предпринимаются; эта работа должна продолжаться в приоритетном порядке. Следующие предложения могут послужить отправной точкой для дополнительного глубокого анализа.

Сокращение риска нанесения ядерного удара в результате просчета

Необходима новая политика и стратегия, направленная на сокращение риска нанесения ядерного удара в результате просчета.

- **Необходимо разработать меры по увеличению времени приятия решения с учетом киберугроз, стоящих перед системами раннего предупреждения.** Кибер-вмешательство в ядерные системы увеличивает риск ложного предупреждения о ядерном нападении и потери уверенности в достоверности информации, необходимой руководству страны для принятия решения об ответном ударе. Никакие возможные усовершенствования в мерах обеспечения кибербезопасности подобных систем не дадут руководству полной уверенности в том, что киберугроза сведена к нулю. Увеличение времени принятия решения (в т.ч. возможные изменения в боеготовности) может оказаться единственным способом компенсировать риски, связанные с киберугрозой.

  На сегодняшний день американские и российские ракеты, поддерживаемые в состоянии высокой боеготовности, могут быть запущены и долететь до своих целей в течение всего нескольких минут – причем после того, как ракета уже запущена, отозвать ее обратно невозможно. У руководства страны может быть всего несколько минут между получением предупреждения о запуске противником ракет и ядерными взрывами на своей территории. Поэтому руководство стремится сохранить возможность оперативного нанесения ответного удара сразу после получения предупреждения о ракетном нападении противника. В разгар кризиса или в момент повышенной напряженности это может привести к поспешной отдаче приказа о нанесении ответного удара из-за ложной тревоги. Все это увеличивает риск применения ядерного оружия в результате просчета. Единственная ошибка может привести к ядерной катастрофе.

  Растущая киберугроза безопасности ядерных вооружений лишь усугубляет существующий риск, поскольку она повышает вероятность выдачи ложного предупреждения об атаке и потери уверенности в достоверности получаемых данных. Военным следует разработать и предложить политическому руководству варианты увеличения времени принятия решения без ущерба для способности страны эффективно отреагировать на ядерное нападение в случае необходимости. В рамках этих вариантов необходимо обеспечить наличие эффективных систем и процессов, которые позволят подтвердить или опровергнуть данные, получаемые от систем раннего предупреждения и других источников, чтобы принять правильное

"Система ядерного управления является незаслуженно обойденным вниманием четвертым элементом ядерной триады. Без высоконадежной и высокоскоростной системы коммуникаций между президентом США, его советниками и теми, кто выполняет задачи ядерного сдерживания, остальные три элемента этой триады окажутся бесполезными. Поэтому с учетом роста угрозы кибератак по всему миру нам следует уделять повышенное внимание защите четвертого элемента триады от этой угрозы."

—Джеймс Виннефелд, адмирал ВМФ США в отставке
ЧЛЕН АНАЛИТИЧЕСКОЙ ГРУППЫ]

решение об ответных действиях. США также нужно сотрудничать с другими странами, чтобы достичь взаимопонимания и предпринять обоюдные шаги по увеличению времени принятия решения.

- **Необходимо выработать нормы, ограничивающие применение кибероружия против ядерных вооружений.** Кибер-вторжение в ядерные системы другого государства может привести к серьезному кризису, даже если само вторжение было непреднамеренным. Если руководство пострадавшего от вторжения государство сочтет, что такое вторжение было прелюдией к обезглавливающему удару по его средствам ядерного сдерживания, то в ответ оно может отдать приказ о применении ядерного оружия. Ввиду возможных последствий такого просчета военное и политическое руководство, а также официальные лица на более низком уровне, должны четко понимать, что кибератаки, нацеленные на ядерные системы, могут привести к непреднамеренной катастрофе, и реагировать соответствующим образом. Верификация выполнения любых норм по ограничению кибер-активности, нацеленной на ядерные системы вооружений, будет весьма сложной задачей. Тем не менее, такие нормы способны снизить вероятность подобного кризиса, особенно в периоды повышенной напряженности. При этом следует учитывать, что выработка подобных норм существенно затруднена двойным (ядерным/неядерным) характером многих систем, связанных с ядерными вооружениями и могущих стать целью кибератак, а также практикой интеграции и размещения ядерных и неядерных систем на одних и тех же объектах (см. вставку на стр. 18 [please check page number as it's likely to have changed due to Russian text expansion]). Существование таких международных норм имело бы положительный результат даже несмотря на то, что они, скорее всего, не остановят негосударственных игроков. К примеру, если эти нормы согласованы на международном уровне, то в случае кибератаки на ядерные системы, предпринятой в нарушение таких норм, подозрение с большей вероятностью падет именно на негосударственных игроков, а это поможет не допустить потенциально опасной международной эскалации.
- **Необходимо повышение выживаемости и надежности ядерных систем**

и процессов управления и связи. Принцип ядерного сдерживания основан на обоснованном предположении, что атакуемое государство сможет нанести ответный удар либо в ходе первоначальной атаки, либо после нее. Киберугроза делает выживаемость ядерного оружия, средств их доставки и систем управления и связи еще более важной и сложной задачей. Системы управления и связи должны обладать устойчивостью к киберугрозе, чтобы у руководства была возможность оставаться на связи с ядерными системами (как для получения, так и для передачи данных), друг с другом (для принятия обоснованного решения об ответных мерах) и с иностранными партнерами (для де-эскалации кризиса).

РЕШЕНИЕ В ХОДЕ НАПАДЕНИЯ?

Один из возможных вариантов продления времени принятия решения, рассмотренных Аналитической группой, заключается в принятии президентов решения под нападением. Другими словами, после получения информации о том, что противник запустил по США ядерные ракеты, президент отдает приказ о нанесении ответного удара по истечении определенного периода времени (к примеру, через 10 часов). При этом выполнение приказа об ответном ударе может быть поставлено в зависимость от выполнения определенных условий – в частности, от подтверждения достоверности предупреждения о ядерном ударе противника, а также от достоверного определения самого противника. Сторонники этого варианта полагают, что он позволит вовремя отменить приказ о нанесении ответного ядерного удара, если предупреждение о запуске противником ракет по США окажется ложной тревогой. Но при этом от также обеспечит нанесение ответного ядерного удара, если предупреждение подтвердится, укрепляя таким образом потенциал сдерживания. Противники данного варианта возражают, что он понизит порог отдачи президентом приказа о нанесении ядерного удара, пусть даже и отложенного. Они также считают, что отмена уже отданного приказа об отложенном нанесении ядерного удара может столкнуться с техническими и процедурными препятствиями. Наконец, они полагают, что если произойдет утечка информации о таком приказе, это само по себе может спровоцировать нанесение ядерного удара по США противоположной стороной. Многие эксперты также высказывали возражения против самой идеи автоматического выполнения приказа без человеческого участия (например, в случае, если президент США окажется не в состоянии исполнять свои обязанности после отдачи приказа об отложенном ударе). Они указывают на то, что такое «автоматическое» выполнение приказа исключит другие варианты пропорционального реагирования на атаку противника, а также создаст юридические проблемы и сложности в плане функционирования цепи передачи приказа. Очевидно, данный вариант требует дальнейшей проработки и обсуждения. Надо также разработать и альтернативные варианты по увеличению времени принятия решений.

Сокращение кибер-рисков, угрожающих системам ядерного сдерживания

Многие из нижеуказанных мер по сокращению рисков для безопасности ядерных вооружений уже внедряются в США (см. вставку на стр. 34) [please check page number as it's likely to have changed due to Russian text expansion]. Правительство США должно и впредь уделять этим мерам повышенное внимание и обеспечивать их должное финансирование. Это крайне важно для сохранения уверенности в должном функционировании ядерного арсенала и поддержания стратегической стабильности.

- **Обеспечение безопасности и диверсификация критических систем.** США инвестируют серьезные ресурсы в меры по защите своей критической инфраструктуры, в т.ч. систем ядерных вооружений, от киберугроз. Хотя ни одно из технических решений не гарантирует 100-процентной защиты ядерных вооружений от киберугроз, необходимо предпринимать все возможные меры по укреплению безопасности и устойчивости соответствующих систем. Важно также принимать меры по увеличению вероятности быстрого обнаружения кибератак и снижению вероятности отказа критических систем в результате таких атак. К числу приоритетов относится сокращение риска отказов, способных привести к нарушениям в работе сразу нескольких систем и платформ.

  В этой связи повышенное внимание следует уделять диверсификации систем и компонентов (ядерных вооружений, средств доставки и систем коммуникаций), а также анализу возможных последствий воздействия киберугрозы на новые, модернизированные, сетевые и автоматизированные системы по мере выполнения программ модернизации ядерного оружия. К числу возможных мер относится сохранение и более широкое использование нецифровых систем; снижение сложности систем; повышение устойчивости спутниковых и других каналов коммуникаций; обеспечение безопасности и диверсификация поставок компонентов в рамках производственной цепи; и усиленные диагностические испытания компонентов. Имеет смысл применять и такие дополнительные меры, как использование динамических решений по укреплению устойчивости критических коммуникационных систем.

- **Повышение приоритета минимизации кибер-рисков в планах модернизации.** Ядерный арсенал США находится на начальных этапах рассчитанной на десятилетия программы модернизации и рекапитализации. В рамках этой программы предусмотрено развертывание новых и модернизированных средств доставки во всех трех компонентах ядерной триады (МБР наземного базирования; баллистические ракеты морского базирования и подводные ракетоносцы; стратегические бомбардировщики). Дополнительные планы также включают модернизацию имеющихся атомных боеголовок, рекапитализация стареющей ядерной инфраструктуры, модернизация американских систем управления и связи, а также повышение эффективности управления всем ядерным комплексом. Поскольку ядерные системы все больше становятся автоматизированными и сетевыми, пропорционально растут и кибер-риски. Поэтому все решения об автоматизации и подключении к сети критических систем ядерного комплекса потребуют нахождения верного баланса между преимуществами

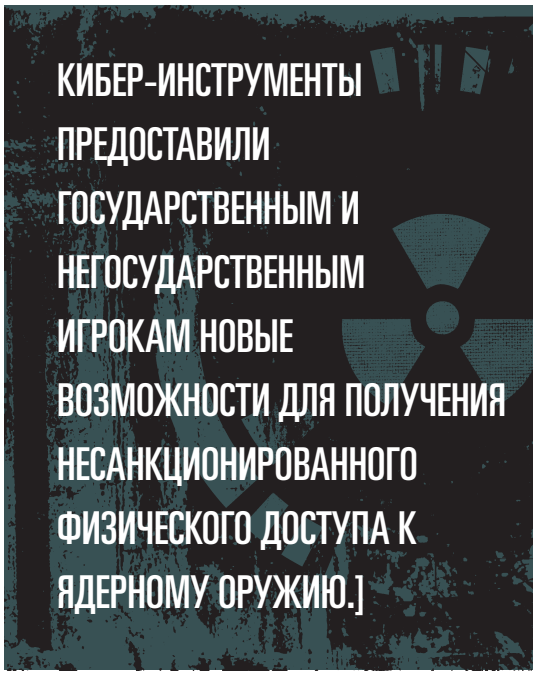
> **"Возможные последствия сбоя в системах управления ядерным оружием девяти государств превосходят по своим масштабам последствия нарушений в работе любых других сложных систем. Лидеры ядерных держав должны выделять и обращать внимание на проблемы, возникающих на стыке неизбежной цифровизации и казалось бы неизменных объектов систем ядерного управления."**
>
> *—Ричард Данциг, бывший секретарь ВМФ США*
> ЧЛЕН АНАЛИТИЧЕСКОЙ ГРУППЫ]

в плане функциональности таких модернизированных систем и потенциальным ростом их уязвимости к киберугрозам. По мере внедрения планов модернизации и рекапитализации будет жизненно важно обеспечить глубокий анализ потенциальных последствий киберугроз для новых и модернизированных систем. Это относится и к модернизации цифровых ядерных систем, которые по нынешним технологическим меркам считаются устаревшими. При модернизации таких систем понадобятся инновационные и строгие меры по обеспечению целостности этих систем и определению угроз, которым они могут быть подвержены. В частности, все новые поставщики, участвующие в процессе модернизации, должны обеспечить должный уровень безопасности.

- **Создание кадрового резерва.** Даже усиленные меры безопасности не могут полностью исключить вероятности «взлома» ядерных систем с помощью кибер-средств. В случае взлома критических ядерных систем решение проблемы и восстановление работоспособности затронутых систем станет наивысшим приоритетом. Для диагностики и эффективного реагирования на кибератаки против ядерных систем потребуется уникальная подготовка и опыт в сфере как информационных технологий, так и ядерного оружия. Правительству США следует вкладывать ресурсы в подготовку соответствующих специалистов. Необходимо также обеспечить наличие списка экспертов в данной области, которые могут быть срочно привлечены в случае чрезвычайной ситуации для обнаружения кибератак против ядерных систем и принятия эффективных контрмер. Подготовку такого кадрового резерва можно начать с организации курсов на уровне колледжей, а также курсов повышения квалификации уже существующих специалистов. Руководство США должно также обеспечить наличие ресурсов для информирования всех операторов, работающих на предприятиях ядерно-оружейного комплекса, о важности кибербезопасности. Человеческий фактор всегда будет одной из главных уязвимостей, которые могут быть использованы любым потенциальным нарушителем. Поэтому помимо обеспечения кадрового резерва необходимы также меры по проверке и другим мерам безопасности в отношении для борьбы с угрозой внутреннего нарушителя; такие меры являются ключевым компонентом защиты ядерных систем от киберугроз.

Сокращение риска несанкционированного применения

Кибер-потенциал предоставил государственным и негосударственным игрокам дополнительные возможности и инструменты для несанкционированного доступа к ядерному оружию с целью его хищения либо несанкционированного применения, что может привести к катастрофическим результатам.



- **Укрепление мер безопасности и физической защиты ядерного оружия, анализ уязвимостей ядерного оружия перед угрозой комбинированных физических/кибер атак.** США следует продолжать внедрение мер по укреплению физической безопасности и кибербезопасности ядерного оружия и средств доставки, в т.ч. систем передового базирования в Европе. Это оружие всегда будет оставаться уязвимым для попыток хищения с применением комбинированных физических и кибер-средств.
  В рамках мер по укреплению безопасности США следует проводить всесторонний и регулярный анализ на предмет того, как киберугрозы потенциально могут усугубить существующие физические угрозы безопасности ядерного оружия. В рамках такого анализа нужно будет определить уровень угрозы, как в настоящем, так и в будущем, по мере развития соответствующего потенциала противников США. Понадобится также определить, какие дополнительные меры безопасности необходимы для минимизации соответствующих угроз. Аналогичные меры следует принять и всем остальным странам, обладающим ядерным оружием.

Применение глобального подхода в сфере киберугроз безопасности ядерных вооружений

Киберугрозы безопасности ядерных вооружений требуют глобального подхода. Все страны, обладающие ядерным оружием, подвергаются риску кибератак, а потенциальные последствия применения ядерного оружия вследствие просчета или несанкционированного применения, равно как и последствия потери эффективности всей системы ядерного сдерживания, будут иметь глобальный масштаб. Для лучшего понимания глобальной природы данной угрозы, а также для выработки глобальных подходов к сокращению этой угрозы необходимо предпринять следующие шаги.

- **Инициировать двусторонний диалог с Россией.** В качестве первого шага США следует инициировать двусторонний диалог с Россией на тему киберугроз ядерному оружию (в т.ч. угрозы вмешательства со стороны третьих сторон) для достижения взаимопонимания по вопросу потенциального влияния киберугроз на систему сдерживания и стратегическую стабильность. Необходимо начать переговоры с целью выработки общего понимания нашей взаимной заинтересованности в

минимизации соответствующих рисков и определения практических двусторонних и многосторонних мер. Эти шаги должны включать в себя выработку норм относительно кибератак против ядерных вооружений, а также соглашение о практических мерах по укреплению стабильности.

- **Укрепление международного сотрудничества в сфере сокращения киберугрозы.** Без двустороннего и многостороннего сотрудничества по вопросу киберугрозы односторонние меры по укреплению безопасности ядерных вооружений могут быть восприняты другими странами как дестабилизирующие. Поэтому крайне важно вести двусторонний и многосторонний диалог как с ядерным державами, так и со странами, не обладающими ядерным арсеналом. На ранних этапах особенно важен будет диалог с Россией и Китаем. Конечно, обсуждение таких вопросов со странами, которые сами по себе являются источником киберугроз, будет сложным с политической и технической точки зрения. Однако стоящая перед нами киберугроза слишком серьезна, чтобы избегать взаимовыгодного диалога в сфере экзистенциальных национальных интересов, и актуальна она как для Соединенных Штатов, так и для противников США.

  В рамках двустороннего и многостороннего диалога следует рассмотреть нормы и правила поведения в данной сфере – например, договоренность воздерживаться от кибератак против ядерных вооружений. Также было бы полезно рассмотреть односторонние и взаимные меры по сокращению риска применения ядерного оружия в результате кибератак. В частности, США следует искать возможности для международного сотрудничества по повышению эффективности и надежности систем раннего предупреждения, в т.ч. путем взаимодействия по линии военных ведомств. Это поможет снизить вероятность выдачи ложных предупреждений о ядерном нападении в результате успешной кибератаки. Наконец, США следует также работать как независимо, так и с другими государствами с целью разработки более эффективных инструментов верификации, которые помогут укрепить доверие к будущим мерам контроля над кибер-вооружениями и соглашениям и мерам по укреплению доверия.

ЗАКЛЮЧЕНИЕ

Самое смертоносное оружие на планете уязвимо перед лицом кибератак, последствия которых могут быть глобальными и катастрофическими. Сценарии, рассмотренные в данном докладе, указывают на тревожную реальность: кибератаки способны подорвать уверенность американского военного руководства в собственной способности контролировать свои ядерные силы и средства. Государства, вооруженные ядерными арсеналами, должны осознать серьезность данной угрозы и принять все возможные меры противодействия, в т.ч. путем внесения изменений в собственную ядерную политику и доктрины. Такие шаги жизненно необходимы для обеспечения гарантированного контроля государств над собственными ядерными вооружениями и связанными с ними системами.

Одних лишь технических мер для эффективного сокращения этой угрозы недостаточно. Киберугроза безопасности ядерных вооружений также требует мер более широкого характера, направленных на снижение связанных с кибератаками рисков применения ядерного оружия в результате просчета либо несанкционированного применения. Подобные изменения также должны быть направлены на поддержание уверенности в эффективности всей системы ядерного сдерживания. Данный доклад рекомендует принять целый ряд мер, направленных на решение приоритетных задач в сфере сокращения киберугрозы безопасности ядерных вооружений. Он может послужить отправной точкой для более глубокого анализа. Рекомендуется, в частности, продлить время принятия решений с учетом киберугрозы системам раннего предупреждения; разработать нормы, ограничивающие использование кибер-оружия; обеспечить безопасность и диверсификацию критических систем; а также изучить возможности для выработки глобальных подходов к данному вопросу, основанных на международном сотрудничестве.

Киберугроза и кибер-потенциал государственных и негосударственных противников постоянно эволюционируют, требуя динамичных и постоянно эволюционирующих стратегий реагирования. Руководство ядерных государств должно постоянно и тщательно анализировать киберугрозы безопасности своих ядерных вооружений; предметом анализа, в частности, должны стать последствия модернизации ядерных систем. Еще более важной является готовность государственного руководства задаваться вопросом о том, насколько жизнеспособной остается стратегия ядерного сдерживания на данный момент, и не устарела ли она – особенно если сохранение прежней уверенности в должном функционировании ядерных вооружений окажется невозможным. Данный доклад может послужить отправной точкой для того, как правительства могут решать эти вопросы.

СПИСОК ЧЛЕНОВ АНАЛИТИЧЕСКОЙ ГРУППЫ

Мнение экспертов, участвующих в работе данной Аналитической группы, не выражает взглядов и интересов стран и организаций, которые они представляют. Все они принимали участие в работе Группы в личном порядке в качестве экспертов. Участие в работе Группы не подразумевает согласия со всеми аспектами данного доклада и сформулированных в нем рекомендаций. Взгляды, изложенные в докладе, могут не совпадать со взглядами организаций, с которыми связаны члены Группы. Их принадлежность к организациям указана исключительно в справочных целях.

СОПРЕДСЕДАТЕЛИ АНАЛИТИЧЕСКОЙ ГРУППЫ

Эрнест Мониз, сопредседатель и исполнительный директор NTI

Сэм Нанн, сопредседатель NTI

Дес Браун, вице-председатель NTI

ЧЛЕНЫ АНАЛИТИЧЕСКОЙ ГРУППЫ

Джеймс Эктон, сопредседатель Программы по ядерной политике Фонда Карнеги за международный мир

Брук Андерсон, партнер в компании «The Hyalite Group»

Стивен Андерсон, консультант по вопросам национальной безопасности, NTI

Джеймс Картрайт, генерал морской пехоты США в отставке, председатель Группы по вопросам оборонной политики, Центр стратегических и международных исследований

Ричард Кларк, председатель и исполнительный директор, Good Harbor Security Risk Management

Чарльз Кертис, почетный президент NTI и почетный член Совета директоров NTI

Ричард Данциг, старший советник, Лаборатория прикладной физики Университета Джонса Хопкинса.

Эрин Дамбахер, сотрудник Программы по научно-технических вопросам, NTI

Крис Финан, исполнительный директор, со-основатель и председатель правления, Manifold Technology

Эндрю Фаттер, доцент кафедры международной политики Лестерского университета

Джеймс Гослер, старший научный сотрудник, Лаборатория прикладной физики Университета Джонса Хопкинса, член Научного совета по вопросам обороны

Юджин Хэбигер, генерал ВВС США в отставке, бывший главнокомандующий Стратегического командования США

Мелисса Хасавей, президент компании «Hathaway Global Strategies LLC»; старший консультант проекта по кибер-безопасности Белферовского центра науки и международных дел (Гарвардский университет)

Аарон Хьюз, старший научный сотрудник Центра стратегических и международных исследований, бывший заместитель министра обороны по кибер-вопросам

Херб Лин, старший научный сотрудник департамента кибер-политики и кибер-безопасности, Центр международной безопасности и сотрудничества, Стэнфордский университет; научный сотрудник Гуверовского института

Джозеф Най, почетный профессор Гарвардского университета, Гарвардская школа им. Кеннеди

Саманта Питтс-Кифер, старший директор, Программа глобальной ядерной политики, NTI

Дебора Планкетт, директор, Plunkett Associates LLC

Джоан Ролфинг, президент и директор по оперативным вопросам, NTI

Брайан Роуз, сотрудник Программы глобальной ядерной политики, NTI

Дебора Розенблум, исполнительный вице-президент, NTI

Линн Растен, старший советник, Программа глобальной ядерной политики, NTI

Скотт Саган, старший научный сотрудник, Институт международных исследований Фримана Спогли, Стэнфордский университет; старший научный сотрудник Центра международной безопасности и сотрудничества, Стэнфордский университет; профессор политологии, Стэнфордский университет

Джеймс Ставридис, адмирал ВМФ США в отставке; ректор Флетчеровской школы юриспруденции и дипломатии, Университет Тафтса

Пейдж Стаутленд, вице-президент по научно-техническим вопросам, NTI

Майкл Сулмайер, директор проекта по кибербезопасности, Белферовский центр науки и международных отношений (Гарвардский университет)

Вильям Тоби, старший научный сотрудник, Белферовский центр науки и международных отношений (Гарвардский университет)

Марк Велланд, профессор нанотехнологий, Центр нанотехнологий, Кембриджский университет

Изабель Вильямс, старший советник, Программа глобальной ядерной политики, NTI

Джеймс Виннефелд, адмирал ВМФ США в отставке; почетный профессор международных отношений, Школа международных отношений им. Сэма Нанна, Технологический институт Джорджии; старший внештатный научный сотрудник, Белферовский центр науки и международных отношений (Гарвардский университет)

ОБ АВТОРАХ

Д-р Пейдж Стаутленд, вице-президент NTI по научно-техническим вопросам, отвечает за научно-технические проекты, направленные на укрепление ядерной безопасности по всему миру. До своего прихода в NTI д-р Стаутленд занимал руководящие должности в Ливерморской национальной лаборатории им. Лоуренса. До этого он работал в министерстве энергетики США в качестве директора Программы химической и биологической национальной безопасности, а также в Лос-Аламосской национальной лаборатории. Имеет степень бакалавра, присужденную Колледжем Сент-Олафа (Норсфилд, Миннесота) и степень доктора химических наук, присужденную Калифорнийским университетом в Беркли.

Саманта Питтс-Кифер, старший директор Программы глобальной ядерной политики NTI, отвечает за проекты NTI в сфере российско-американских отношений, ядерной политики США, северокорейской проблематики и разоружения. В 2012 году она получила степень магистра государственного управления в Школе им. Кеннеди Гарвардского. Работала ассистентом-исследователем Девида Сангера, когда он писал книгу «Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power» («Конфронтация и секреты: тайные войны Обамы и неожиданное применение американской силы»). Питтс-Кифер работала юристом в фирме Simpson Thacher & Bartlett LLP и клерком в штате судьи Апелляционного суда США Мариэн Трамп Барри. Имеет степень бакалавра, присужденную Колледжем Сент-Олафа, а также степень юриста, присужденную Школой юриспруденции Университета Вилланова.

Из предисловия
Эрнест Мониз, Сэм Нанн, Дес Браун

В данном докладе под названием «Ядерное оружие в новую кибер-эпоху: Доклад Аналитической группы по изучению киберугроз безопасности ядерных вооружений» предлагается анализ киберугроз безопасности ядерных вооружений, а также рекомендации, разработанные группой бывших и отставных высокопоставленных правительственных чиновников, военных руководителей и экспертов в сфере ядерных систем, ядерной политики и киберугроз.

Пока идёт работа над совершенствованием технических мер безопасности, все ядерные державы также должны найти ответ на несколько стратегических вопросов. Если мы не можем быть до конца уверены в работоспособности наших систем перед лицом атаки со стороны хорошо подготовленного противника, и если у нас нет полной уверенности в нашей способности контролировать собственные ядерные вооружения, то что это означает для дальнейшей актуальности стратегии ядерного сдерживания? Эта стратегия помогла США и СССР пережить Холодную войну, но не стала ли она опасно устаревшей с наступлением эпохи кибер-войн? И не следует ли нам скорректировать нашу ядерную политику и подходы к развертыванию сил, чтобы свести к минимуму потенциальные риски кибератак?

Мы считаем, что США обязаны взять на себя инициативу в сфере борьбы с киберугрозами безопасности любых ядерных объектов и систем – но особенно это относится к безопасности ядерных вооружений. Именно поэтому основное внимание в данном докладе уделяется США. Дальнейшая работа в рамках этого проекта будет направлена на анализ уязвимостей ядерных систем в других государствах, поскольку предотвращение использования ядерного оружия - как террористами, так государствами, как целенаправленного, так и непреднамеренного – является задачей глобального характера. Все страны, обладающие ядерным оружием и ядерными объектами, должны делать больше, много больше, для обеспечения безопасности своих ядерных вооружений и связанных с ними систем. Слабое звено где бы то ни было может привести к глобальной катастрофе.

NTI
BUILDING A SAFER WORLD
www.nti.org