Маркова А.В. ©
Бакалавр, Нижегородский национальный исследовательский университет им. Н.И. Лобачевского, кафедра Международных отношений, магистратура (кафедра мировой политики и международного права)

ПОСЛЕДСТВИЯ И ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ КИБЕРАТАК КАК ИНСТРУМЕНТА ВНЕШНЕЙ ПОЛИТИКИ ГОСУДАРСТВ НА ПРИМЕРЕ ВИРУСА «СТАКСНЕТ»

Аннотация

В данной статье была сделана попытка проанализировать перспективы ведения войн между государствами в киберпространстве. В качестве примера автор рассматривал эпизод совместной операцией США и Израиля против ядерного объекта Ирана в Нетензе, связанный с заражением автоматизированных систем управления объекта вирусом «Стакснет». Цель исследования - определить, возможно ли ведение кибервойн в будущем. В связи с этим были поставлены следующие задачи: проследить, как произошло заражение ядерного объекта в Нетензе, оценить последствия заражения, установить, какое влияние имели действия США и Израиля на состояние Иранской ядерной программы, а также установить, возможны ли эффективные действия государств в киберпространстве и способны ли они оказать существенное влияние на расстановку сил на международной арене.

Ключевые слова: кибервойна, Иранская ядерная программа, «Стакснет», Нетенз.
Keywords: cyber war, Iranian nuclear program, «Stuxnet», Netenz.

Современный этап развития человечества внес свои коррективы не только в отношения между индивидами, но и трансформировал взаимодействия, происходящие на международном и государственном уровне. В частности, неотъемлемым элементом политики любого государственного актора является информационная сфера.

Следует подчеркнуть, что технический и научный прогресс поднял процессы, происходящие в данной области государственной политики на качественно новый уровень. Говоря об информационной сфере, нельзя переоценить роль Интернета и киберпространства в международных отношениях и мировой политике. Компьютерные технологии оптимизировали способы связи и доставки информации, что значительно облегчило информационный обмен. Однако в связи с подобными тенденциями и явлениями появляются новые угрозы и вызову национальной безопасности государств, к числу которых можно также отнести *кибервойну.*

Данное явление определяется как противостояние в сети Интернет между государствами, или односторонние действия государства, направленные на нарушение работы компьютерных систем госорганов страны-противника, а также иных инфраструктурных систем [9].

Есть основания полагать, что, с течением времени, взаимозависимость информационной среды и иных направлений как внутренней, так и внешней политики современных государств, неуклонно растет. В частности, данный тезис находит свое подтверждение в таких событиях международной среды, как эпизод с разоблачением Эдвардом Сноуденом тайной разведывательной деятельности США, потрясшее мировое сообщество и вызвавшее бурную негативную реакцию.

В данном случае можно обозначить связь между информационной безопасностью и другим направлением политики современных государств, включая ядерную безопасность и оружие. Как информационная среда, так и вопросы обеспечения ядерной безопасности, в сложившихся условиях современности являются актуальными для всех без исключения государств. Данный вопрос становится все более важным в связи со стремительным развитием информационной сферы, инструментов хранения, передачи и обработки данных, что не в

©© Маркова А.В., 2014 г.

последнюю очередь касается ядерной политики государств и иных акторов международных отношений

Принимая во внимание современные тенденциями развития, кибервойна, являясь не только современным вызовом и угрозой национальной безопасности, но одновременно с этим возможным инструментом ведения внешней политики и достижения целей, может оказать существенное влияние на ядерную политику и безопасность. Таким образом, необходимо проанализировать возможность и потенциал использования средств кибервойны в рамках данной политической сферы.

Рассмотрению одного из эпизодов применения средств кибервойны, а именно совместной операции США и Израиля против иранского ядерного объекта в Нетензе, посещена данная статья.

Перед детальным рассмотрением вышеуказанного примера, необходимо охарактеризовать окружающую среду, в которой велось и ведется информационное и ядерное противостояние современных государств.

Считается, что круг основных игроков в сферах ядерной и информационной безопасности включает в себя США, Китай, Россию, Израиль, Иран, Южную Корею. Следовательно, удовлетворение национальных интересов вышеперечисленных государств в области обеспечения ядерной безопасности может быть достигнуто методами информационной войны или противостояния.

Применительно к позиции США необходимо подчеркнуть, что разведка является неотъемлемой частью и ключевым элементом системы государственных органов в их борьбе с транснациональным терроризмом и предотвращением террористических атак [1, 8]. Стоит также отметить, что события 11 сентября 2001 г. заставили руководство США поменять внешнеполитические и стратегические приоритеты. Бывший американский президент Дж. Буш младший объявил войну терроризму [3, 132], что проявилось не только во внешнеполитическом курсе государства, но также повлияло на сбор разведданных, а именно направление работы американских спецслужб.

Было также установлено, что число государств, занимающихся «подозрительной деятельностью» по сбору разведывательной и стратегической информации в 2005 г. составил 43%, по отчетам Совета Безопасности Минобороны США [2, 232]. Более того, американские службы разведки также заботит вопрос о кибератаках. В отчете ФБР от 2005 г. утверждалось, что в Интернете развивается шпионаж, и, несмотря на широкое использование программ защиты, 9 из 10 американских компаний пострадали от шпионских атак в период 2004-2005 гг., что привело к потерям в 67 млрд. долларов в год [4, 334]. Оценки масштабов кибератак в экономической и бизнес сфере позволяют утверждать, что перспективы их использования во внешней политике государств весьма реальны.

Одним из инструментов, применяемых в ходе кибервойны, является так называемее Вредоносное Программное Обеспечение (далее – ВПО), целью которого является дестабилизация или полное выведение из строя инфраструктурной системы того или иного стратегического объекта. Иными словами, проникая внутрь системы, ВПО нарушает работу процессов, обеспечивающих ее нормальное функционирование. Точное и своевременное применение ВПО может нанести непоправимый урон для стратегически важных объектов того или иного государства, затратив при этом минимальный объем людских, военных и денежных ресурсов, о чем можно судить из некоторых примеров использования ВПО, в том числе в области ядерной политики и оружия.

Как известно, наболевшей проблемой мирового сообщества является неразрешенный вопрос о ядерной программе Ирана. Данная проблема активно обсуждалась на заседаниях Международного Агентства по Атомной Энергетике в период с 2006 по 2008 гг. Ряд резолюций, требовавших прекратить дальнейшее развитие Ираном своей собственной ядерной программы, не привели к значительным сдвигам в разрешении иранского кризиса. Правительство страны заявило о намерениях продолжать развивать собственную ядерную программу для удовлетворения внутренних потребностей государства и в интересах иранского народа [6].

Отказ Ирана следовать требованиям МАГАТЭ остановить процесс обогащения урана, изложенным в резолюциях периода 2006-2008 гг., привел к недовольству мирового сообщества, в первую очередь США и Израиля. Заявления о мирном характере иранской ядерной программы также подвергались сомнениям. В результате США и Израиль в условиях секретности начали подготавливать военные варианты предотвращения дальнейшего развития ядерного потенциала противника [8].

Однако позднее стало очевидно, что военный удар мог бы понести за собой множество отрицательных последствий, требовал весьма больших усилий, а также не имел явных оснований, вследствие чего было решено начать поиск иного выхода из сложившейся ситуации. Дальнейшие меры по выводу из строя атомных объектов Ирана должны были стать частью длительной операции США под названием «Олимпийские Игры», начатой еще при администрации Дж. Буша младшего. Стоит отметить, что кампания велась в сотрудничестве с Израилем по оперативным и стратегическим соображениям: США нужен был доступ к тайной израильской разведывательной сети в Иране, кроме того, Штаты хотели убедить Израиль отказаться от авиаудара по Ирану [8].

Применение новейшего оружия кибервойны стало частью данной операции. «*Стакснет*» («Stuxnet» – англ.) – ВПО, примененное совместно США и Израилем против Ирана с целью подорвать дальнейшее развитие ядерной программы последнего. Далее будет рассмотрено, какие последствия имел данный эпизод как для политики Ирана, США и Израиля, так и для обстановки на международной арене в целом.

С февраля 2007г. центром иранской ядерной программы становится Нетенз, где к середине 2009 г. было установлено более 8 тыс. центрифуг (при максимальной вместительности в 50 тыс.). Работу всех составляющих контролировали АСУ (Автоматизированные Системы Управления), чью работу обеспечивал промышленный комплект средств автоматизации компании «Сименс» Simatic Step 7, работающий на платформе Microsoft Windows. Сбой в работе АСУ неизбежно привел бы к нарушению работы всего объекта.

Так как защита системы предотвращала воздействие через Интернет, возможной причиной проникновения ВПО на объект должен был послужить банальный человеческий фактор. Однако стоит отметить, что точный путь заражения АСУ объекта в Нетензе остается загадкой. Известно, что инфекции «Стакснета» были направлены на пять разных промышленных предприятий Ирана, которые занимались АСУ и подозревались в нарушении условий нераспространения [5]. Неразборчивость и неосторожность персонала привела к тому, что ВПО проникло в систему, распространяя дальнейший ущерб в автоматическом режиме.

Алгоритм действия «Стакснета» можно свести к следующему. При попадании в систему, вирус инициирует наличие определенного программируемого логического контроллера (ПЛК), который, в свою очередь, соединен с определенным типом преобразователя частоты [6]. Инспекторами МАГАТЭ было установлено, что максимальная скорость, которую может выдержать ротор центрифуги IR-1 на объекте в Нетензи, составляет 1400 Гц, а в обычном режиме и вовсе не превышает показателя в 1064 Гц. «Стакснет» делал так, что вначале скорость увеличивалась до 1410 Гц (в течение 15 минут), затем вновь достигала нормального показателя в 1067 Гц (на 27 дней), далее подала до 2 Гц (на 50 минут), показателя слишком низкого для продолжения обогащения, затем вновь возвращалась к номинальной скорости в 1067 Гц на те же 27 дней. Цикл мог повторяться бесконечно [6]. Первоначально стояла задача незаметно привести к износу составляющих системы, т.е. в первые два месяца добиться хронической усталости в каскадах. «Стакснет» должен был работать незамеченным в течение нескольких месяцев, маскируя сигналы тревоги с выходящих из строя центрифуг.

Нет сомнений в том, что функционал червя был бы неполным без обратной связи с центром. Так одной из функций «Стакснета» были отчеты с описанием зараженных им компьютеров и сообщения о выявлении на них ПО Simatic. Данные серверы управления могли также отсылать обратно инструкции о дистанционном вызове процедур на зараженных компьютерах объекта или обновления ПО из главного окна. «Стакснет» также мог проникать сквозь брандмауэры и в машины, не имевшие прямого доступа к Интернету [12].

Безусловно, организация подобного вторжения требует тщательной подготовки и велась совместными усилиями АНБ (Агентство Национальной Безопасности) США и израильской организацией технической разведки, известной, как «Часть 8200». Более того, Израиль предоставил свой ядерный объект Димона для репетиции вторжения. Специалисты занятые в операции также должны были обладать богатой компетенцией в вопросах ядерной инженерии, АСУ, обогащения урана и разведывательных операций. Очевидно, что Разведывательная подготовка к «Олимпийским играм» началась за годы до атаки «Стакснет» с виртуальной разведки сетей Нетенза.

С технической точки зрения, подготовка вторжения не была сложной, хотя и требовала определенных усилий. Разработчикам АНБ пришлось задействовать так называемые уязвимости нулевого дня Microsoft Windows, т.е. ранее неизвестные уязвимости системы, которые возможно использовать для осуществления атаки. Тем не менее, было необходимо провести тщательные испытания кода, для чего требовался доступ к центрифугам IR-1, ПО Simatic и периферийным устройствам Нетенза [12].

Свидетельством длительной и тщательной подготовки к вторжению является то, что еще в 2003 г. США получили быстродействующую внутреннюю память аналога IR-1, а именно – ливийской центрифуги P-1. Кроме того, несомненным преимуществом США являлся тот факт, что сама компания «Сименс» в 2008 г. сотрудничала с Национальной Лабораторией Айдахо. Таким образом, США имели доступ к нужному тестовому оборудованию [6]. Для обхода механизмов антивирусной защиты некоторые модули (драйверы) ВПО имели цифровую подпись, сделанную с использованием сертификатов компаний Realtek и JMicron, которые, предположительно, были украдены.

Несмотря на все предпринятые усилия, тщательную подготовку и дестабилизирующее действие «Стакснета», говорить об успехе операции нужно весьма осторожно. Оценивая результаты проникновения вируса, необходимо исходить из целей, преследуемых США и Израилем в рамках данной операции. Как уже было сказано выше, они заключались в замедлении темпов развития ядерной программы Ирана. Таким образом, необходимо оценить последствия воздействия червя на АСУ объекта в Нетензе.

По отчетам МАГАТЭ, «Стакснет» заставил иранцев заменить тысячу центрифуг к январю 2010 г. [15]. При этом отчеты показывают, что объем производства низкообогащенного урана в Нетензе вырос с 80 до 120 кг в месяц за время атаки с середины 2009 до средины 2010 г. В причинах таких противоречивых данных необходимо разобраться, чтобы оценить масштаб и эффективность воздействия червя на АСУ станции.

С одной стороны, «Стакснет» выполнил свои основные задачи. Вирус проник через иранскую сетевую защиту и действовал незаметно в течение нескольких лет, постепенно и поступательно нарушая работоспособность центрифуг. Воздействие червя привело к хронической деградации процесса обогащения урана на объекте.

Целью американских и израильских спецслужб было убедить иранцев в своей несостоятельности. Иными словами, они хотели заставить думать Иран, что сбои в работе станции были вызваны внутренними причинами. В некоторой мере это удалось создателям червя: на атомном объекте начали увольнять людей и был установлен жесткий контроль над всеми происходящими процессами [7, 125].

С другой стороны, стоит отметить следующие факторы, ставящие под сомнения результаты действий АНБ и «Части 8200». Несмотря на то, что целью «Стакснета» была не полная остановка производства обогащенного урана, а лишь замедление его темпов, эффективность работы червя весьма проблематично оценить.

Во-первых, по оценкам инспекторов МАГАТЭ, станция работала неэффективно. Причина кроется в ошибках, которые существовали в самих установках и центрифугах: из отчетов МАГАТЭ видно, что уровень ошибок составлял 10%. Это больше показателя «Стакснета» всего лишь на 1,5%. Тенденция к снижению объемов переработки газа наблюдала еще до вторжения, в 2008 г. [15].

Кроме этого, сотрудники Агентства не обнаружили каких-либо изменений самого производительного каскада в Нетензе (модуль A24), а тысяча отключенных центрифуг

относилась к строящимся каскадам (модули A26 и a28), которые работали в вакууме, но не содержали газа гексафторида урана. Таким образом, во время атаки были выведены из строя пустые центрифуг Нетенза.

В свою очередь, когда к августу 2010 г. в широкий доступ были выложены «заплаты» для «Стакснета», число центрифуг вновь начало расти и объем перерабатываемого газа вырос соответственно. Однако после начала нормальной и полной работы станции, его объем достиг показателя до вторжения [6].

В целом, «Стакснет» промахнулся мимо основных целей в Нетензе, обогащение продолжалось и усиливалось во время атаки, а иранцы полностью устранили ущерб. Наконец, 9 июля 2010 г. специалисты белорусской антивирусной компании «ВирусБлокада» обнаружили в Иране вредоносное программное обеспечение (ВПО), которому было названо Stuxnet. Как известно, секретность в случае работы взломщика - необходимое условие, которое и было нарушено при обнаружении вируса. Несмотря на ограничения в распространении, «Стакснет» все-таки просачивался за пределы Ирана, что давало сообществу информационной безопасности множество образцов для изучения.

С другой стороны, данный пример дал понять мировому сообществу, что традиционные проблемы международных отношений могут быть рассмотрены с новых позиций, а для их решения применены новейшие инструменты внешней политики, к которым можно причислить и *кибервойну.*

Исходя из сомнительных результатов операции США и Израиля можно прийти к выводу, что, в отличие от традиционных войн, где достаточно правильно выбрать цель для нанесения удара, задача виртуальных технологий комплексная и более сложная. Мы можем определить несколько задач, стоящих перед противниками в кибервойне, а именно: собрать детальную развединформацию о механических и организационных характеристиках своей цели, получить доступ к ее компьютерной сети, исследовать ее уязвимости для прокладки маршрута к автоматизированной системе управления и активировать специально разработанную «боевую нагрузку» для подрыва цели.

Несмотря на то, что вирус был обнаружен и результаты проникновения «Стакснета» на иранский объект не оправдали ожиданий разработчиков, становится очевидным, что перспективы ведения крупномасштабных кибервойн вполне реальны. Можно смело утверждать, что подобные кибератаки продолжаться и будут применены для решения стратегически важных задач современных государств и обеспечения их национальных интересов.

Литература

1. Старкин С.В. – Анализ разведывательной информации по транснациональному терроризму в современных внешнеполитических условиях: подходы американских теоретиков // Гуманитарные исследования. – 2011. №1. – С. 6-12.
2. Старкин С.В. – Борьба с распространением ОМП как проявление трансформации глобальных угроз в деятельности американского разведывательного сообщества // Гуманитарные и социальные науки. – 2011. № 2. – С. 232-230.
3. Старкин С.В. – Влияние геополитической среды на трансформацию контрразведывательной парадигмы спецслужб США // Вестник Брянского Государственного Университета. – 2011. №2. С. 130-134.
4. Старкин С.В. Проблемы типологизации разведывательной информации в американском теоретическом дискурсе // Вестник Нижегородского университета им. Н.И. Лобачевского. – 2011. № 1. – С. 329-335.
5. Дмитриевски И. Ядерная программа Ирана приторможена вирусом Stuxnet // Stop-News [Электронный ресурс]. – Режим доступа: http://stop-news.com/857-yadernaya-programma-irana-pritormozhena-virusom-stuxnet.html
6. Albright D., Brannan P., Walrond C. – Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment// Institute for science and national security [Электронный ресурс]. – Режим доступа: http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/
7. Dinnis H.H. – Cyber Warfare and the laws of war // Cambridge University Press. 2012. 337 c.

8. Heller O. – Transferring the War to the Enemy's Computer // Israeldefense [Электронный ресурс]. – Режим доступа: http://www.israeldefense.com/?CategoryID=483&ArticleID=2708
9. Martin C. Libicki – Cyberdeterrence and cyberwar // Project Air Force [Электронный ресурс]. – Режим доступа: http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf
10. Morteza R. – What's the Best Defense against Stuxnet? A Comparison of Which Tools are the Best for Finding Stuxnet in a System // Control Magazine Web Exclusive, 28 May 2012 [Электронный ресурс]. – Режим доступа: http://www.controlglobal.com/articles/2012/stuxnet-iranian-view.html
11. Raas W., Long A. Osirak Redux? Assessing Israeli Capabilities to Destroy Iranian Nuclear Facilities // International Security. Spring 2007. № 31:4 [Электронный ресурс]. – Режим доступа: http://web.mit.edu/ssp/publications/working_papers/wp_06-1.pdf
12. Sale R. – Stuxnet Loaded by Iran Double Agents // Industrial Safety and Security Source. 2012 [Электронный ресурс]. – Режим доступа: http://www.isssource.com/stuxnet-loaded-by-iran-double-agents
13. Yong W. – Iran Says It Arrested Computer Worm Suspects // New York Times, 10 Oct. 2010 [Электронный ресурс]. – Режим доступа: http://www.nytimes.com/2010/10/03/world/middleeast/03iran.html?_r=0
14. IAEA, Implementation of the NPT Safeguards Agreement and Relevant Provisions of Security Council Resolutions 1737 (2006), 1747 (2007), 1803 (2008) and 1835 (2008) in the Islamic Republic of Iran. GOV/2010/10, 18 Feb.2010 [Электронный ресурс]. – Режим доступа: http://www.iaea.org/Publications/Documents/Board/2009/gov2009-35.
15. Iran: Nuclear Intentions and Capabilities // Office of the Director of National Intelligence, Nov. 2007 [Электронный ресурс]. – Режим доступа: http://www.dni.gov/files/documents/Newsroom/Press%20Releases/2007%20Press%20Releases/20071203_release.pdf