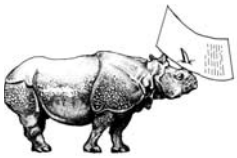

Олег Демидов, Елена Черненко

ГРОЗНЫЙ УМ НА СТРАЖЕ КИБЕРБЕЗОПАСНОСТИ

Из последних разоблачений бывшего сотрудника американских спецслужб Эдварда Сноудена стало известно, что США тайно разрабатывают программу *MonsterMind*, позволяющую не просто купировать кибератаки, но и в автоматическом режиме наносить ответные удары по предполагаемому агрессору. В условиях, когда атаки можно осуществлять через территорию третьих стран, а эффективных межгосударственных мер доверия в киберпространстве нет, такая программа может привести к серьезному конфликту.

ПРО ОТ КИБЕРАТАК

Получивший убежище в России бывший сотрудник АНБ и ЦРУ Эдвард Сноуден в середине августа 2014 г. в одной из московских гостиниц тайно встретился с репортерами американского журнала *Wired*. Казалось, он уже рассказал журналистам все, что знает о слежке американских спецслужб за пользователями Интернета. Однако в ходе интервью Э. Сноуден впервые поведал о разрабатываемой АНБ программе под кодовым названием *MonsterMind*. Программа должна отслеживать начало кибератак по целям на территории США и купировать их. Такие программы существуют уже много лет, но, по словам Э. Сноудена, у *MonsterMind* будет уникальная особенность: система сможет наносить ответный *удар* в автоматизированном режиме, т. е. без вмешательства человека.

Э. Сноуден решил рассказать о *MonsterMind* прежде всего потому, что, по его словам, принцип работы этой программы нарушает права граждан США. Дело в том, что, для того чтобы программа вычислила атаку и отбила ее, необходимо проанализировать все потоки данных. «А если мы анализируем все потоки информации, то это означает, что мы должны их все перехватить. А это, в свою очередь, означает, что мы нарушаем четвертую поправку к конституции США, которая запрещает произвольные обыски и аресты, перехватывая частные переговоры без ордера, без явной причины и даже без подозрений наличия нарушений», — пояснил он *Wired*.

Между тем такие программы, как *MonsterMind*, могут привести к куда более серьезным последствиям, чем нарушение чьего-то права на тайну личной жизни. Источник кибератаки крайне сложно отследить, поскольку диверсии могут осуществляться с использованием инфраструктуры третьих стран. Если же программа будет наносить ответные *удары* в автоматическом режиме, пострадать может безвинная сторона. Об этом предупреждает и сам Э. Сноуден: «К примеру, кто-то может находиться в Китае и создать видимость, что атака исходит из России. Тогда ответный удар может быть нанесен, скажем, по больнице в России. Что произойдет?».

Ущерб от такой ответной атаки может быть существенным. В 2006 г. вредоносная программа удалила информацию с серверов одной из больниц Чикаго, в результате чего работа учреждения была фактически парализована — все данные о пациентах хранились в электронном виде. В 2009 г. в результате кибератаки на один из госпиталей Далласа была надолго выведена из строя система кондиционирования — и это при температуре в +40 °С. По мере растущей компьютеризации медицинских учреждений они неизбежно будут становиться более уязвимыми для угроз из киберпространства.

В целом же, по данным Международного комитета Красного Креста, кибератаки против критически важной гражданской инфраструктуры могут оставить тысячи человек без воды, еды и электричества, а диверсии против атомных электростанций и дамб — технически они тоже возможны — могут привести к жертвам.

КИБЕРПРО В ОТНОШЕНИЯХ РОССИИ И США

Казалось бы, России нечего опасаться в связи с появлением у США таких программ, как *MonsterMind*, поскольку в прошлом году эти страны заключили первые в мире договоренности о мерах доверия в киберпространстве, своего рода *пакт об электронном ненападении*. Речь идет о пакете из трех межправительственных соглашений «О мерах укрепления доверия в сфере использования информационно-коммуникационных технологий (ИКТ)», подписанных президентами России и США В. В. Путиным и Бараком Обамой на полях саммита *Большой восьмерки* в июне 2013 г. Речь, в частности, идет об установлении между Москвой и Вашингтоном *горячих линий* по предотвращению перерастания киберинцидентов в полномасштабный кризис — аналоге запущенного в советское время прямого канала связи для снижения рисков в ядерной сфере.

В рамках договоренностей 2013 г. был даже задействован ключевой элемент системы предотвращения ядерной войны. Речь идет о созданных в 1987 г. национальных центрах по уменьшению ядерной опасности (НЦУЯО). Они работают круглосуточно, позволяя военным России и США уведомлять друг друга о проведении ракетных испытаний, чтобы они не были восприняты как акт агрессии, как это едва не случилось в 1983 г., когда накануне учений НАТО *Able Archer* («Опытный лучник») произошло ложное срабатывание советской системы предупреждения о ядерном нападении. Сегодня возможности этих центров параллельно используются и для взаимных уведомлений об атаках на объекты критической информационной инфраструктуры.

Линии связи и обмена информацией о компьютерных инцидентах организованы еще на двух уровнях. Первый — между кураторами вопросов национальной безопасности. Этот канал может быть задействован в случае возникновения кризисной ситуации, требующей немедленного информирования президентов. Второй — между группами экстренной готовности к компьютерным инцидентам (CERT), которые *мониторят* вредоносную активность в сетях. В июне 2014 г. спецпредставитель президента России по вопросам международного сотрудничества в сфере информационной безопасности А. В. Крутских сообщил, что эти каналы связи уже доказали свою эффективность (по его словам, они, в частности, были задействованы при подготовке к зимней Олимпиаде 2014 г. в Сочи)[1].

Между тем на разработку этих соглашений ушло почти два года. О самой сути мер доверия стороны договорились довольно быстро, но процесс затянулся из-за терминологических разногласий. США говорили о мерах доверия *в сфере ИКТ*. Россия настаивала на другой формулировке — *в сфере использования ИКТ*. Несущественная на первый взгляд разница имела принципиальное значение. Вашингтон делал упор на физической защите своих компьютерных систем, Москва же хотела обезопасить от вредоносного использования ИКТ, чтобы не стать жертвой очередного вируса типа *Stuxnet*, но одновременно и не допустить превращения новых

технологий в оружие для информационных войн. Договориться удалось только после череды хакерских атак на американские банки в августе 2012 г. (Вашингтон заподозрил в их организации Иран). В итоге в название президентского заявления вошел российский вариант формулировки, а в его текст, как и в три сопутствующих межправительственных соглашения, оба варианта.

Наряду с *горячими линиями* эти соглашения предусматривали и создание рабочей группы по сотрудничеству в киберпространстве в рамках российско-американской президентской комиссии. Предполагалось, что она займется дальнейшим усовершенствованием двусторонних мер доверия в этой сфере. Сопредседателем группы с российской стороны является замсекретаря Совбеза России С. М. Буравлев, а с американской — координатор Белого дома по вопросам кибербезопасности Майкл Дэниел. Однако из-за событий вокруг Украины США минувшей весной приостановили свое участие в президентской комиссии, заморозив и работу новой группы (ее участники успели провести лишь одно заседание).

Горячие линии по предотвращению киберинцидентов продолжают работать, несмотря на разногласия по Украине. Однако у Москвы и Вашингтона теперь по сути нет площадки, где можно было бы обсудить механизмы взаимодействия на момент, когда *MonsterMind* будет введена в строй. Ведь *горячие линии* могут предотвратить эскалацию киберинцидентов, только если решение о нанесении ответного удара по предполагаемому агрессору принимается человеком. Если, к примеру, находящиеся на Ближнем Востоке террористы *Исламского государства Сирии и Леванта* выведут из строя дамбу в США, а следы атаки будут указывать на сервер в Омске, американцы — в соответствии с имеющимися соглашениями — должны связаться с коллегами в России, прежде чем принимать решение об ответных действиях. *MonsterMind* этого делать не будет.

Особых надежд нет и на Организацию по безопасности и сотрудничеству в Европе (ОБСЕ) — еще одну площадку для выработки мер доверия в киберпространстве. Переговоры по заключению между членами этой организации многостороннего соглашения также длились почти два года и в какой-то момент зашли в тупик из-за терминологических споров. В итоге лишь в декабре 2013 г. Совет министров ОБСЕ одобрил *Первоначальный перечень мер укрепления доверия с целью снижения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий*.

ALUMNI ПИР-ЦЕНТРА

ГАЛИЯ ИБРАГИМОВА (к.п.н., консультант ПИР-Центра):
Бархатные и *оранжевые* революции в странах СНГ, *Арабская весна* на Ближнем Востоке, гражданская война на востоке Украины и противостояние России и Запада — часто эти события приводятся в доказательств того, как сильно и как часто кибер- и информационные технологии влияют на безопасность в мире. Но интернет ли виноват во всех этих событиях? Да, посредством него организовывалось общение участников революций, люди выходили на площади, отстаивали свою точку зрения. Но не кибертехнологии виноваты в изживших себя политических системах в некоторых странах СНГ, где имели место революции. Не интернет — причина убийства Муаммара Каддафи. Не на информационных технологиях лежит ответственность за то, что мир за много лет так и не приблизился к ядерному нулю. Причина всему — не холодное *железо* технологий, а сознание — не всегда чистое и отдающее себе отчет — людей, которые определяют ход событий. Кибер- и информационные технологии — это скорее проводник гениальных и ничтожных, разумных и опасных идей. В зависимости от того, в чьих руках оказываются эти технологии, они становятся *машиной смерти* или *зерном созидания*. Но мир стоял до интернета и, надеюсь, выстоит и сейчас, лишь бы человеческий разум восторжествовал!

Таких мер доверия в документе 11. В частности стороны договорились: «делиться соображениями по различным аспектам национальных и транснациональных угроз в сфере ИКТ и их использования»; «облегчать сотрудничество между национальными компетентными органами и обмениваться информацией»; проводить консультации, чтобы снизить вероятность ошибочного восприятия и возможного возникновения политической или военной напряженности либо конфликта в результате использования ИКТ и обеспечить защиту важнейших объектов национальной и международной ИКТ-инфраструктуры». Правда, все это предполагается делать на сугубо добровольной основе и лишь в той мере, в которой это комфортно каждой из сторон. От возможных негативных последствий таких программ, как *MonsterMind*, эти меры не спасут.

Российская сторона надеялась, что этот перечень — не зря он назван *первоначальным* — станет основой для выработки куда более субстантивного и обязательного к исполнению, однако из-за украинского кризиса и на этой площадке переговорный процесс застопорился. Между тем вслед за США и другие страны стремятся обзавестись программами, позволяющими отвечать киберагрессорам в автоматическом режиме. Недавно Министерство обороны Великобритании объявило тендер (на сумму £2 млн) на создание системы, по описанию похожей на *MonsterMind*.

ГЛОБАЛПРО В КИБЕРПРОСТРАНСТВЕ

Три года назад Россия начала продвигать в ООН инициативу, направленную на принятие свода норм поведения в киберпространстве (в рамках концепции конвенции «Об обеспечении международной информационной безопасности»). Среди требований Москвы — призыв предотвратить милитаризацию киберпространства. Однако пока страны обсуждали российскую инициативу (или скорее выдвигали альтернативные перечни правил), большинство технологически развитых государств начали разрабатывать не только средства киберзащиты, но и вооружения. Говорить о запрете кибероружия, таким образом, уже поздно. Но еще можно попытаться предотвратить его автоматизированное применение.

Важно понимать, что именно взаимное доверие и обмен информацией, а не сдерживание и обоюдное наращивание потенциалов представляют собой тот ресурс двусторонних и многосторонних действий, который способен сдержать нарастание риска крупных столкновений в киберпространстве, а в итоге — глобального киберконфликта. Здесь стоит вернуться к аналогии безопасности в сфере использования ИКТ и стратегической ядерной стабильности, которая обрела популярность во второй половине нулевой декады усилиями прежде всего американского экспертного и военно-управленческого истэблишмента. Подразумевалось, что столкновения с участием государств и их посредников в киберпространстве имеют свои особенности, но в целом подчиняются базовой логике сдерживания. Иначе говоря, имеется возможность управлять эскалацией конфликта, выстраивать стратегию его удержания в неких ограниченных рамках, либо, напротив, планировать и осуществлять упреждающий удар на ранней стадии, не оставляющий шансов на контрудар противнику.

На практике же вся действительность последних лет доказывает тот простой факт, что четкое управление конфликтом в киберпространстве едва ли возможно. Можно взять классический пример со *Stuxnet*, который замышлялся как предельно узконаправленное и целевое средство киберсаботажа, а в итоге после *утечки* в Сеть распространился (хотя и без последствий) на многие сотни устройств в разных странах мира, а также послужил базой для создания ряда вредоносных программ, включая *DuQu*. Более того, сегодня в заимствованиях функционала и концепции *Stuxnet* эксперты обвиняют уже инструментарий нового поколения, поражающий западные сети и АСУ ТП (кампания *Energetic Bear* и вредоносное ПО *Dragonfly*).

Еще один фактор, в корне подрывающий возможность управления киберконфликтом с позиций управления эскалацией и сдерживания, — анонимность его субъектов. Все чаще СМИ и лица, принимающие решения, ошибаются при первой (срочной в условиях конфликта) оценке авторства атаки — взломы промышленных и финансовых сетей в Японии автоматически приписываются КНДР, хотя потом следы уводят в Китай, и т. п. Массированные, охватывающие многие десятки стран кампании кибершпионажа, увенчавшиеся похищением терабайт чувствительных данных, такие как *Red October*, после раскрытия просто растворяются в воздухе. С управляющих серверов подается команда на самоуничтожение червя в зараженных системах, большая часть цифровых отпечатков стирается крайне хитроумными модулями вредоносного ПО, и исчезает возможность не только силового или правового ответа на такую акцию, но и определения круга причастных субъектов в принципе.

ALUMNI ПИР-ЦЕНТРА

МАКСИМ СИМОНЕНКО (стажер-исследователь Центра комплексных европейских и международных исследований НИУ–ВШЭ): Программа *MonsterMind* показала, что практика может идти впереди теории в сфере кибербезопасности. До сих пор никто не научился определять реальный источник атак в киберпространстве с вероятностью 100%. Но как тогда можно создать автоматизированную систему реагирования, если даже неизвестно, кто инициировал атаку? Путем проб и ошибок в бою. Решение реальных проблем, с которыми сталкиваются люди при минимизации ущерба от кибератак, придаст дополнительный импульс к созданию инструментов идентификации источника кибератак.

Но, пожалуй, самое парадоксальное отличие использования ИКТ в стратегических и военно-политических целях от применения ОМУ — все более заметная инфляция его применения. В какой-то момент, приблизительно совпавший с первыми сообщениями о *Stuxnet*, могло показаться, что осмысление ИКТ как военно-политического ресурса движется в сторону *последнего довода королей* — средства, годящегося для случаев, когда конвенциональные средства давления, в том числе силового, недостаточны, но все же применяемого на практике в отличие от атомной бомбы. Сегодня *MonsterMind* и целый набор подобных программ, исследований и инициатив в силовых министерствах и *мозговых центрах* США, Великобритании, Израиля, Франции, Китая, России и еще многих государств — яркое свидетельство невостребованности этого сценария.

Концепция подобных разработок — ведение *проактивных* действий в киберпространстве в штатном режиме, т. е. конфликт как *modus operandi*. Вопрос о том, чем *проактивная оборона* отличается от нападения, может иметь смысл для военных аналитиков и теоретиков международных отношений, но для инженеров, программистов, задающих режим работы и спектр функций подобных систем, он отнюдь не очевиден. Как многократно отмечалось различными авторами, эффективная стратегия кибероборонs невозможна без сканирования чужих сетей, выхода за рамки собственного периметра, получения доступа к третьим системам, поиска уязвимостей в чужом периметре и т. д.

Миллионы попыток обхода установленной защиты, постоянный поиск слабых мест, фиксируемый одним лишь Пентагоном в отношении своих сетей ежедневно, — лишнее подтверждение этого тезиса. Кибероружие по большей части утратило роль средства сдерживания, поскольку его техническая сущность и направление эволюции сегодня сводятся к систематическому, постоянному применению. Помимо технологии этому сильно способствуют два уже упомянутых фактора: 1) его крайне низкая ресурсоемкость, полная восполнимость, дешевизна, относительная материальная и интеллектуальная доступность; 2) крайне низкий риск несения международной (либо иной) ответственности за его применение. В итоге барьер, удерживающий политико-управленческий аппарат от принятия решения о запуске

очередной кампании кибершпионажа либо разработке и запуске в эксплуатацию очередного средства *проактивной кибероборонь*, крайне размыт и неочевиден.

Означает ли девальвация принятия решений об использовании ИКТ в военно-политических целях размывание угрозы, проистекающей от таких действий? Ни в коем случае. Никто не отменил того факта, что рост зависимости критической инфраструктуры, как гражданской, так и военной, от ИКТ и Интернета, продолжается просто как закономерность технического прогресса. Достаточно упомянуть глобальный тренд на *Smart Grid*, не говоря уже о наступлении *Интернета вещей* за рамками вопросов критической инфраструктуры. Кроме того, никто еще не испытывал полные возможности кибersаботажа на практике, заимствуя терминологию американского генералитета, *цифровой Пёрл-Харбор* все еще не случился, поскольку *Stuxnet* было явно недостаточно.

Таким образом, пока международное сообщество, несмотря на выдающиеся усилия России, в сфере использования ИКТ параллельно с ростом глобальной взаимозависимости и сотрудничества остается в состоянии, близкому к гоббсианской *войне всех против*. Что можно сделать, чтобы минимизировать стратегические риски такого формата взаимодействия, если эффективное силовое сдерживание невозможно, как и всеобщее *цифровое разоружение*? Вероятный ответ лежит в русле двусторонних российско-американских наработок и инициатив в рамках ОБСЕ — выстроить систему взаимных мер доверия с тем, чтобы сделать поведение ее участников более открытым и предсказуемым друг для друга.

Одно из слагаемых взаимной выгоды такого решения состоит в том, что даже если стороны не снимают все противоречия и не отказываются от всех попыток поиска слабых мест друг друга, страховочная сетка мер доверия по крайней мере: а) снижает риски неконтролируемой эскалации конфликта; б) повышает ресурс нейтрализации негативных действий третьих сторон. Если уж Пентагон создает автоматизированную систему ответа на кибератаки, становятся крайне востребованы человеческая коррекция и верификация ее работы, в том числе на основе данных извне. Вот здесь уместен пример ядерной эры — к идее обмена данными между НЦУЯО СССР и США подтолкнули в том числе ошибки автоматизированных систем обнаружения пусков баллистических ракет, лишь в последний момент скорректированных человеком.

Конечно, и здесь нельзя не согласиться с последовательной позицией МИД России, преимущества такого инструментария растут пропорционально числу примыкающих к нему акторов и становятся максимальными в случае реализации глобальной системы мер доверия. При этом приоритет должен уделяться, как это и происходит в случае России–США, не юридическим гарантиям безопасности, а именно техническим механизмам обмена информацией об атаках, аномалиях трафика, инцидентах компьютерной безопасности и т. д. Проблематика использования ИКТ в контексте международной безопасности еще ждет своего Джона Нэша и убедительной теории взаимовыгодных игр в киберпространстве, но, как представляется, взаимные меры доверия должны занять в ней важное место.

Примечания

[1] Мы за интернационализацию управления Интернетом. *Газета Коммерсантъ*, 16 июня 2014 г., http://kommersant.ru/doc/2492013?isSearch=True (последнее посещение — 2 августа 2014 г.).