Вохминцев Игорь

Мифы и реальность кибервойны

Вступление

Мировое сообщество вступает в новый этап. Символика этого выражается двумя фигурами, продолжая идеи Дж. Розенау о туристе и террористе[1] и Дж. Аарона о солдате и дипломате[2], можно с уверенностью сказать, что появилась еще одна пара - пользователь и хакер.

За последние тридцать лет роль Интернета в мире значительно выросла. Сегодня Интернет превратился в полноценную арену международного противостояния. Эта тема скрыта от посторонних глаз, но, как любой запретный плод, привлекает. После разоблачений Э. Сноудена и появления у стран одного за другим армейских подразделений, ведающих «кибервойной», это тема стала ещё более привлекательной. Индустрия развлечений активно эксплуатирует её, снимая фильмы и делая игры, в которых киберовойна показана неправдиво. Это создает огромное количество мифов, а понимание реальной ситуации важно для политиков и дипломатов в силу специфики их работы и обязанностей. Подавляющее большинство из них имеет гуманитарное образование, что не предполагает знания того, как на самом деле функционирует Интернет-среда. Цель этой работы - дать краткое представление о том, что такое кибервойна. Перед тем как начать, нужно сделать необходимую ремарку. До сих пор нет ни единого понятия, ни определения того, что понимается под кибервойной. Это область, где смешались частные корпорации, обычные хакеры-одиночки, спецслужбы, регулярные армии, террористические группы и обычные пользователи.

Поле боя

Обычно описание любых войн начинается с мест, где они происходили. Место, где проходит кибервойна, часто называют пятой областью войны в одном ряду с сушей, морем, воздухом и космосом. Самая важная характеристика этой области – её непрерывность. Каждое устройство, подключенное к сети связано со всеми остальными. Конечно, мы немного лукавим, когда говорим, что преград нет. Ведь сразу приходят в голову логины и пароли, антивирусы, знаменитый «китайский файрволл». Но горы, океаны и моря — это совсем не то же самое, что антивирус или брандмауэры. Одна из крупнейших десантных операций в мировой истории - высадка в Нормандии - потребовала огромных вложений, человеческих, финансовых, политических и временных ресурсов, и все это для переброски людей и оружия через относительно небольшое водное пространство — Ла-манш. Атака в Интернете сегодня может быть проведена небольшой группой людей, которые не будут рисковать своей жизнью, и атака потребует гораздо меньше денег в сравнении с произведённым эффектом, чем высадка в Нормандии. Например, в 1999 году 15-летний Джонатан Джеймс получил незаконный доступ к компьютерам НАСА и Пентагона[3]. Конечно, компьютерная сеть Пентагона не отключилась, но представьте себе такой же случай в период холодной войны! США и СССР тратили в свое время миллионы долларов и рублей, чтобы получить гораздо меньше информации путем классической разведки! Более того, в 5-й области очень сложно оценить характеристики классических сил противника: технику, количество людей, оборудование и т. д. Небольшие государства,

группы людей и отдельные лица в этом пространстве могут играть важную роль[4], когда обладают специальными умениями и они хотят причинить вред своем противнику. Еще одна характерная черта - невозможность отличить военную сферу от гражданской. В Интернете нет разделения на фронт и тыл, все пространство — это поле боя или, лучше сказать, серая зона, негражданская и невоенная. С технической точки зрения и гражданские, и военные используют одни и те же системы и оборудование. Нет разницы между ноутбуком, который используется в кибер-подразделениях армий и ноутбуком рядового пользователя. Они работают на одинаковых протоколах. Да, военные используют уникальное ПО, но, как показывает практика, рынок специализированного ПО широк и плохо контролируется по сравнению с нелегальным рынком летального оружия. Яркий пример вирус-шифровальщик «WannaCry», но о нем будет сказано ниже. Кроме того, как видно на примере операции «Внутренняя решимость» (операция армии США и их союзников против ИГИЛ* (*Организация, запрещенная на территории Российской федерации) на территории Сирии) ВВС США использовали гражданские смартфоны и специальные приложения (ATAK Kit) на базе операционной системы Android для координации бомбардировок, которые также частично доступны для гражданского населения[5]. Проблема технологий двойного назначения стоит остро. Более того, гражданские сети могут использоваться как прокси (посредники) для кибератак. Это представляет собой наиболее серьезную проблему атрибуции врага в киберпространстве. Любой ноутбук, ПК, любая сеть могут быть использованы для атак, а затем снова возвращены к гражданской жизни, и даже владелец может не знать, что его компьютер, например, используется для DDoS-атак (об этом типе атак подробнее ниже). Атака может быть осуществлена через любую сеть, и защитить все - невыполнимая задача[6].

Сила

Теперь перейдем к основной составляющей всех войн и конфликтов - силе. Силовое превосходство - главный постулат войны. Это было теоретически и практически обосновано в начале 19 века прусским офицером Клаузевицем, в фундаментальном труде «О войне», который не потерял актуальности и сегодня, в котором он пишет о важности превосходства в силе для победы. В те времена сила измерялась преимущественно количественных показателях (больше солдат, пушек, ядер). Это было абсолютом тактики и стратегии Первой и Второй мировых войн и это привело к гонке вооружений во время холодной войны, когда на первый план начали выходить качественные показатели силы (более совершенное оружие). На этом основана теория сдерживания, MAD (взаимное гарантированное уничтожение) и политика разрядки. Но в киберпространстве другое отношение к понятию силы. Основы войны в киберпространстве основываются не на наращивании силы, как это происходит в традиционных конфликтах, а на способности находить слабые места врага. Конечно, атака преобладает над защитой, но эффективная атака — это изучение противника, поиск слабых мест и удар по ним. Такое положение дел обусловлено характеристиками объектов и средств нападения. Компьютерный код — это не стена, и, как и в обычной войне, использование более мощной пушки против более толстой стены здесь не поможет. Код можно сравнить с лесом, и сколько бы вы в него ни стреляли, даже из самого мощного оружия, никакого вреда он не принесет. Но зная порядок расположения деревьев и их вид можно пройти через лес. Поиск и использование уязвимостей, изучение врага - основа войны в киберпространстве. Оружие этого измерения

эксклюзивно и, как правило, может быть использовано один раз. Попробуем провести аналогию для объяснения эксклюзивности. Отметим, что, как и любая другая, она не лишена недостатков, в процессе упрощения теряются тонкости и профессионалам она может показаться неподходящей. В обычном конфликте танк может стрелять по пехоте, бронетехнике и укрепленным позициям противника. В киберпространстве танков нет, но есть вредоносное ПО. Нет смысла использовать вредоносную программу для атаки на конкретную уникальную систему (а это те, которые используются в сфере национальной безопасности), для которой она не предназначена. Вредоносная программа может просто не работать. Примером является Stuxnet, который активировался самостоятельно только в определенной системе и был неактивен в других. Иран беспокоился о безопасности своей ядерной программы и система управления центрифугами, которые обогащали уран была изолирована от Интернета, но была связана с другими сетями, которые были связаны с большим количеством других и с Интернетом. Вирус был внедрён в одну из таких систем и постепенно перепрыгивал из одной в другую, пока не дошёл до ядерных объектов Ирана и вывел их из строя[7]. Во-вторых, после того, как атака была обнаружена, атакованные обнаруживают уязвимость системы, которая использовалась для атаки, закрывают эту уязвимость, и вторая попытка атаки на эту же самую уязвимость завершится неудачей. Злоумышленник должен разработать новое вредоносное ПО, а это требует нового большого количества ресурсов. Следует отметить, что все вышесказанное касается в первую очередь военных систем и критической инфраструктуры страны. А нападения на такие объекты требуют серьезных вложений денег, времени и сил. Есть исключение из правила эксклюзивности атакующего агента - DDoS-атаки, в основе которых лежит максимально возможное наращивание сил. Если говорить простыми словами, то в основе такой атаки лежит создание чрезмерной нагрузки на сеть через большое количество запросов, таким образом, сеть становится недоступной. Это можно сравнить с ситуацией, когда на почту одномоментно приходит столько посылок и писем, что специалисты не справляются с их обработкой и доставкой и закрывают почтовое отделение.

Как и на что нападают?

Все многообразие вариантов ведения войны в киберпространстве можно классифицировать по цели, которая преследуется. Такой подход кажется вполне логичным. Давайте сразу откажемся от цели простого заработка, поскольку мы говорили, что это простая афера. В данном контексте финансово мотивированные атаки не рассматриваются, так как выходят за рамки рассматриваемого в эссе предмета. Хотя зарабатывание денег составляет большинство случаев среди всех киберпреступлений!

Во-первых, целью атаки могут быть сами данные. Атака на компанию в сфере цифровых технологий «Solar Winds» это идеально демонстрирует[8]. Хакеры получили доступ к личным данным клиентов компании, среди которых как частные, так и государственные структуры. Почтовая переписка, личные данные — всё оказалось скомпрометировано. Как показало расследование, атака готовилась тщательно. Она началась в сентябре 2019 года с момента тестового внедрения вредоносного кода, но широкой публике о ней стало известно только в конце 2020 начале 2021. Но с уверенностью можно сказать, что подготовка началась до сентября 2019, ведь эта дата фактического начала атаки. Этот пример идеально демонстрирует всю ту сложность и временные интервалы, которые нужны для планирования и проведения атаки. Это совершенно

непохоже на кино, где требуются 10 минутные беспорядочные удары по клавиатуре для взлома системы.

Еще одна особенность заключается в том, что большинство компьютерных заражений в мире происходит через фишинговые рассылки и социальную инженерию. То есть без использования технических средств, а только через изучение личности жертв и поиск их слабых мест. Эти методы также использовались Киберкомандованием США[9]. В 2016 году им была проведена операция «Сияющая симфония» против ИГИЛ* (Организация, запрещенная на территории России). При её проведении активно использовались методы социальной инжинерии и весьма успешно. Всем чиновникам, госслужащим и дипломатам необходимо знать правила гигиены информации при работе с компьютером и важными документами, даже если компьютер подключен не к Интернету, а только к локальной сети.

Во-вторых, целью атаки также может служить оборудование, находящееся под контролем компьютера. В этом случае информация также подвергается атаке, но это не важно само по себе, потому что это всего лишь код, а не данные. Атака осуществляется с использованием тех же инструментов и той же стратегии: путем обнаружения уязвимости и внедрения вредоносного кода. Чаще всего таким атакам подвергаются системы, предназначенные для сопровождения работ в режиме реального времени, сбора, обработки, отображения и архивирования информации, удаленного управления процессами (диспетчерское управление и сбор данных, SCADA). Ярким примером является вирус Stuxnet, который использовался для порчи газовых центрифуг для добычи урана на заводе в Иране. Подробно о нём сказано выше. Таким образом, даже изолированные локальные сети также могут оказаться под угрозой. Это обусловлено указанными выше особенностями среды, а именно непрерывностью, а также эксклюзивностью атакующей программы, которая продемонстрировала свою активность в строго определенных условиях (система управления центрифугами). Это можно сравнить с миной, которая перед срабатыванием думает, нужно это делать или нет. Об этом могут мечтать генералы обычных армий. Вернёмся к упомянутому выше примеру операции США «Сияющая Симфония». Почему Киберкомандование США нацеливалось на конкретную информацию, а не на само оборудование, как сделали это организаторы Stuxnet (серверы хранения данных), чтобы полностью обезглавить террористов в Интернете? Атаки на оборудование имеют одно ограничение. Дело в том, что Интернет устроен таким образом, что сайт или страница в социальной сети, доступ к которому вы хотите ограничить, может находиться на одном сервере с сайтами госучреждений, онлайн-магазинов, банков и вы, конечно, не хотите повредить им. А атака по серверу и блокировка доступа могла спровоцировать ограничение доступа к другим сайтам на сервере, не говоря уже о глобальных социальных сетях. Именно эта ошибка была допущена во время блокировки доступа к Telegram[10].

Разведка стоит обособленно. В век тотальной цифровизации огромное количество информации хранится в цифровой форме. Поэтому научная, техническая, политическая, экономическая и военная разведка активно используют цифровые технологии в своих целях. По статистике именно на эту территорию приходится большая часть противостояния в киберпространстве[11]. Не менее интересен пример тотального сбора информации, а не охоты только за секретной информацией. Программа PRISM показала, что такой сбор технологически возможен и осуществляется. PRISM — это государственная программа

разведки США по массовому сбору информации (звонки, Интернет, геоданные)[12]. Впервые мировая общественность узнала о ней в 2013 году. Также стоит учитывать рост технологий и возможностей обработки больших массивов данных.

Нельзя обойти стороной атаку WannaCry, хотя мы и говорили, что не будем рассматривать кибератаки с целью получения прибыли, которой WannaCry и является. Эта атака интересна с другой точки зрения. Вирус использовал уязвимость в системе, проникал и зашифровал все данные, после требовал деньги за расшифровку. Сам компьютер, сервер или ноутбук не пострадали, вирус удаляли после полной очистки системы, но данные пропадали безвозвратно. Компьютеры во всем мире пострадали от этого. Персональное устройство не позволяло получить доступ к личной информации[13]. Также стоит упомянуть особенности такой программы. Очень сложно заставить их атаковать только вашего врага и не касаться ваших систем. Несмотря на уровень современных технологий, никто не может однозначно сказать, как поведет себя программный код. Есть версия, что WannaCry изобрели американские спецслужбы, но украли и использовали злоумышленники[14]. Пострадали и американские компьютеры. WannaCry использовал конкретную уязвимость в широко распространенной системе. Таким образом, подобные программы имеют много общего с химическим оружием. Как только ветер дует не в ту сторону, газовая атака превращается в самоубийство. Это идеальный пример того, насколько «секретные» технологии кибервойны близки к обычной жизни и то, что они легко утекают и их оборот никак не регулируется.

Кибервойна в реальности

Во-первых, кибервойна не похожа на перестрелку. Это больше похоже на игру в шахматы. Во-вторых, кибератака не является идеальным оружием. Приведенный выше пример операции кибер-подразделений американской армии «Сияющая симфония» демонстрирует ограничения. Многие аккаунты террористов в социальных сетях были заблокированы, информация уничтожена. Некоторые из них использовались для диверсий. Они продолжали работать, но американские офицеры были авторами, которые сознательно дискредитировали террористов через их собственные страницы, потому что подписчики этих страниц никуда не делись. Это максимум, на что США могли рассчитывать, готовя столь всеобъемлющую атаку. Большая часть времени и денег была потрачена на подготовку, анализ системы и привычек. К сожалению, террористы перешли на другие платформы и снова создали свои страницы. Только международное сотрудничество может нанести им большой вред, если все основные социальные сети примут правила модерирования опасного контента. И мир к этому идёт, хотя и не так быстро, как хотелось бы. 15 мая 2019 года в Париже состоялась международный саммит Christchurch Call to Action Summit по борьбе с экстремистским контентом. В нём приняли участие правительства и частный сектор[15].

Поэтому в самом начале серьезного конфликта мы увидим мощные обмены кибератаками либо попытки таких атак на важнейшие системы жизнеобеспечения государства, включая сферу услуг, и далее останется разведка и поиск новых незначительных уязвимостей в компьютерных системах противника. Такое развитие событий возможно, но не обязательно. Недавняя история показывает другой и более вероятный сценарий: единичные масштабные кибератаки. Вирус Stuxnet проявлял свою

активность только в системе управления центрифугами, и не проявлял себя в других системах. По сравнению с обычным оружием цель не имеет большого значения для пули или ракеты, чего нельзя сказать об этом вирусе. Интересным случаем смешения кибератаки и атаки обычными средствами является превентивный ракетный удар Израиля по одному из зданий киберподразделения ХАМАС, в котором по версии израильских спецслужб готовилась кибератака на израильскую инфраструктуру[16].

Рядовые пользователи и в первую очередь госслужащие должны быть предельно внимательными, сидя за своими рабочими компьютерами, подключенными к государственным системам и базам данных. Более того, как показано выше, вирусы могут проникать даже в изолированную от Интернета в локальную систему через сторонние сети и внешние физические устройства. А как показывает пример с атакой на Colonial Pipeline[17], один из важнейших нефтяных трубопроводов США, достичь желаемого эффекта можно без атаки на управляющие системы (SCADA). Атака была осуществлена на периферийную компании сеть, с которой были украдены данные, и она была зашифрована, но компания решила остановить весь трубопровод для снижения рисков, вызвав тем самым заметный кризис с поставками топлива на восточном побережье США.

---

[1]Rosenau, James N. « Le touriste et le terroriste ou les deux extrêmes du continuum transnational. » Études internationales, volume 10, numéro 2, 1979, p. 219–252. https://doi.org/10.7202/700940ar

[2]Freymond, Jacques. Revue Historique 233, no. 2 (1965): 511–14. http://www.jstor.org/stable/40950007.

[3] Teen Gets 6 Months for Hacking NASA https://apnews.com/f9cf77e46698af771960d3352883a40a

[4] Cyberdeterrence and cyberwar / Martin C. Libicki. https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

[5] Wasser, Becca, Stacie L. Pettyjohn, Jeffrey Martini, Alexandra T. Evans, Karl P. Mueller, Nathaniel Edenfield, Gabrielle Tarini, Ryan Haberman, and Jalen Zeman, The Air War Against the Islamic State: The Role of Airpower in Operation Inherent Resolve. Santa Monica, CA: RAND Corporation, 2021. https://www.rand.org/pubs/research_reports/RRA388-1.html

[6] Cyberdeterrence and cyberwar / Martin C. Libicki.

[7] Stuxnet в деталях: «Лаборатория Касперского» публикует подробности атаки на ядерный проект Ирана https://www.kaspersky.com/about/press-releases/2014_stuxnet-v-detaliakh

[8] Как происходила атака на SolarWinds https://www.securitylab.ru/blog/company/AngaraTech/350173.php

[9] USCYBERCOM After Action Assessments of Operation GLOWING SYMPHONY https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony

[10] История блокировки Telegram в России https://tass.ru/info/8761201

[11] Hodgson, Quentin E., Logan Ma, Krystyna Marcinek, and Karen Schwindt, Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace. Santa Monica, CA: RAND Corporation, 2019. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2961/RAND_RR2961.pdf.

[12] NSA Office of the Inspector General Releases Three Reports 17 February 2016 https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/3IGReports-Sealed.pdf

[13] Эпидемия шифровальщика WannaCry: что произошло и как защититься https://www.kaspersky.ru/blog/wannacry-ransomware/16147

[14] The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/

[15] https://www.christchurchcall.com/

[16] What Israel's Strike on Hamas Hackers Means For Cyberwar https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/

[17] Back to Basics: A Deeper Look at the Colonial Pipeline Hack https://www.govtech.com/sponsored/back-to-basics-a-deeper-look-at-the-colonial-pipeline-hack