Третья мировая в третьем тысячелетии

А. ГОЛЫШКО, канд. техн. наук, г. Москва

О третьей мировой войне мы говорим уже больше 60 лет, т. е. начали практически сразу же по окончании второй мировой. Много раз она вот-вот начиналась, но каждый раз нам всем везло, и противостоящие стороны демонстрировали "бег на месте". Тем временем наступил XXI век, и война постепенно началась, но уже в виртуальном мире, который создала сеть Интернет, где каждый потенциально не только связан, но и может воевать с каждым. Почему война? — А чем обычно занимаются воюющие стороны? — Разведкой, дезинформацией, разработкой наступательных и оборонительных операций, а также непосредственно контактом с противником, его уничтожением и захватом пленных. Всё это наблюдается сегодня воочию, и есть пострадавшие и даже павшие на поле боя. Просто происходит всё не так громко и не с такими материальными разрушениями. Но происходит. Под прицелом не только отдельные граждане, но и целые сети, коммерческие и оборонные учреждения и, конечно, правительства разных стран. И все они обороняются и даже переходят в контрнаступление. В общем, где-то совсем рядом с нами идёт настоящая кибервойна, отголоски которой регулярно доносятся до нас из всех средств массовой информации. Вот согласно последним мониторинговым данным компании Barracuda Labs, в социальной сети Twitter примерно каждый сотый файл является злонамеренным, тогда как в Facebook — каждое 60-е сообщение.

Антивирусная компания Symantec опубликовала недавно предупреждение компаниям крупного бизнеса о существенном увеличении количества таргетированных (т. е. целенаправленных) атак со стороны как хакеров, руководствующихся экономическими мотивами, так и со стороны так называемых "госхакеров", в задачи которых входит промышленный шпионаж и саботаж. Отмечается и тенденция по взлому небольших компаний, работающих с крупными клиентами, чтобы после взлома малого предприятия иметь возможность атаковать его партнёра. Кстати, за последние 12 месяцев более 30 млн человек в России в той или иной степени пострадали от хакеров, а ущерб, нанесённый злоумышленниками, оценивается примерно в 2 млрд долл. При этом 39 % пользователей соцсетей становились жертвами киберпреступлений.

Летом компания Appthority представила отчёт о том, что 96 % iOS-приложений и 84 % Android-приложений могут получать доступ к конфиденциальной информации пользователя (контактные данные, календарь, местоположение и пр.). И когда сотрудник даже просто приносит на работу собственный смартфон, планшет или другое мобильное устройство, он подвергает предприятие дополнительным рискам безопасности.

Чарли Миллер, исследователь из компании Accuvant, занимающейся разработкой решениий для обеспечения информационной безопасности, предложил метод заражения Android-смартфона вредоносным кодом с помощью технологии NFC, что и было продемонстрировано в рамках хакерской конференции Black Hat в Лас-Вегасе. По словам Миллера, его метод будет работать практически на любом смартфоне, в котором есть поддержка NFC, для чего используются ошибки в операционной системе Android. Для заражения мобильного устройства жертвы с поддержкой NFC хакеру достаточно поднести к нему на расстояние нескольких сантиметров собственный подготовленный смартфон либо электронное устройство с NFC-чипом, после чего в устройство жертвы будет записан вредоносный код. Работу Миллера облегчила сама Google: по умолчанию в Android технология NFC и функция на её основе Android Beam включены. Они автоматически принимают и загружают любой файл, включая web-ссылку, с устройства, с которым связываются.

Генеральный директор некоммерческого альянса International Cyber Security Protection Aliance (ICSPA) Джон Лионс говорит, что в большинстве стран Африки, Восточной Европы, Латинской Америки и других развивающихся регионах нет необходимых юридических структур, созданных для борьбы именно с киберпреступностью, но что ещё хуже, их критически важная инфраструктура плохо защищена от ИТ-нападений, а многие предприятия, работающие в сфере энергетики, водоснабжения, управления транспортом и пр., не взаимодействуют с независимыми ИТ-экспертами, не обмениваются опытом друг с другом и в целом не уделяют должного внимания своей кибербезопасности, чем, скорее всего, и воспользуются как местные, так и зарубежные хакеры. В ICSPA говорят, что считают целесообразным, если промышленно-развитые страны окажут поддержку развивающимся странам в получении экспертизы, связанной с ИТ-защитой критически важных инфраструктурных объектов.

Командование ВМС Индии создало особое управление операциями по обеспечению безопасности различных средств связи, включая космическую, с начальником в звании контр-адмирала, который одновременно станет помощником главкома ВМС. Необходимость в такой организации появилась после недавнего инцидента в штабе Восточного командования индийских ВМС в г. Висакхапатнам, где военные тайны передавались под видом безобидной дружеской переписки разведке потенциального противника.

Управление правительственной связи Великобритании (GCHQ), специализирующееся на радиоэлектронной разведке, объявило о создании первого британского научно-исследовательского института в сфере кибербезопасности. Это "виртуальная организация", в работе которой принимают участие учёные из семи британских вузов. В последнее время оборонные подрядчики и министерства Великобритании неоднократно становились объектами успешных кибератак, и терпение правительства лопнуло. Теперь GCHQ будет консультировать руководство крупнейших компаний лондонского Сити, чтобы помочь частному сектору защититься от киберугроз.

По данным Минобороны США, количество атак на государственные сети стабильно растёт с 2001 г. Основной поток атак приходится на разрозненные хакерские группы, пытающиеся похитить данные, которые потом можно будет продать.

США стали первым государством, которое в 2009 г. объявило о намерении создать кибервойска — специальный военный отдел. Он будет заниматься отражением атак со стороны других государств на правительственные вычислительные сети. Эта инициатива была поддержана Евросоюзом. В марте 2012 г. вице-премьер России Дмитрий Рогозин сообщил, что аналогичная идея обсуждается и в российской власти.

Почти год назад Пентагон впервые заявил о своей готовности к проведению атакующих действий в киберпространстве в ответ на "значительные кибератаки", которые могут угрожать безопасности США. Он готов к "наступательным кибер-операциям" в случае соответствующего приказа президента в ответ на враждебные действия со стороны каких-либо государств или организованных групп. Об этом говорилось в соответствующем докладе Минобороны США, представленном Конгрессу. Враждебными действиями представители Пентагона считают все "значительные кибератаки, направленные против экономики США, правительства или армии страны". О правилах ведения кибервойны умалчивается. По словам аналитиков, новые заявления Пентагона вполне укладываются в существующую политику правительства США, однако готовность к ведению кибервойны никогда ранее не декларировалась так чётко, как сейчас.

Одной из основных сторон официальной стратегии Пентагона в киберпространстве является важность предотвращения атак путём создания защиты, способной перекрыть все основные уязвимости, которые обычно используются в кибератаках злоумышленниками. В новом докладе Пентагона говорится, что группы, угрожающие США сокрушительными кибератаками, будут, мягко говоря, "брать на себя серьёзный риск". Более того, Пентагон "сохраняет за собой право реагировать на агрессию собственными атаками в киберпространстве и других областях". Такая стратегия, кстати, имеет давнюю историю.

Джеймс Е. Картрайт младший, недавно ушедший в отставку вице-председатель Объединённого комитета начальников штабов, ранее уже заявлял, что стратегия США в киберпространстве окажется провальной из-за преобладания в ней оборонительных мер и отсутствия наступательных. Ещё ранее, в июне 2009 г., министр обороны США Роберт Гейтс подписал указ, согласно которому в рамках Пентагона было создано Кибернетическое командование (Cyber Command) для защиты военных компьютерных систем и проведения операций США в киберпространстве (штаб-квартира располагается в Форт-Миде, штат Мэриленд). На вопрос, будут ли сотрудники Кибернетического командования также проводить какие-либо атакующие действия в киберпространстве, представители Пентагона ранее отказывались давать прямые ответы. Однако теперь понятно, что нападение — это лучшая защита.

Всему есть причины, и как, в частности, было сообщено на закрытых слушаниях в Конгрессе США, компьютерные хакеры (в этом подозревают китайских военных) смогли несколько раз инфицировать американские спутники через наземные станции в Норвегии. Доступ хакеров к системе контроля спутников позволит атакующему сделать со спутником всё, что угодно, вплоть до уничтожения. Кроме того, атакующий может незаметно манипулировать спутниковыми данными, чтобы законный владелец аппарата получал искажённую информацию. Спутник дистанционного зондирования Земли Landsat-7 стал жертвой хакеров в 2007 г. и 2008 г., когда злоумышленники фактически захватили контроль над аппаратом "более чем на 12 минут". Аппарат Terra AM-1 также был дважды захвачен хакерами — в июне 2008 г. и октябре 2009 г. на две и более девяти минут соответственно. Правда, в черновике отчёта, который попал в прессу, ничего не говорится о том, что именно делали хакеры со спутниками, когда те находились под их фактическим контролем.

В целом власти США уже в течение последних 5—6 лет обвиняют китайское правительство в организации кибератак и взломе компьютерных сетей с целью получения государственных и коммерческих тайн. Впрочем, ни разу виновные в реальном проведении подобных атак не были задержаны, а сам официальный Пекин отрицает участие страны в таких операциях. При этом американское правительство регулярно обвиняет китайские компании-поставщики телекоммуникационного оборудования в наличии различных преднамеренных уязвимостей и закладок. Как бы отметили бывшие сотрудники советского ВПК или спецслужб, уж кому-кому, но не американцам заниматься такими обвинениями. Разумеется, здесь присутствует и защита собственного рынка связи от внешней экспансии. Но есть, очевидно, и что-то ещё, о чём будет сказано ниже. Американские военные эксперты говорят, что в Китае военизированные хакерские подразделения возникли примерно десять лет назад, однако тогда в их задачи входило подавление интернет-присутствия запрещённой религиозной группировки Фалуньгун. В свою очередь, МИД КНР заявляет, что китайское правительство активно сотрудничает с другими странами в борьбе против киберпреступников.

Агентство Национальной Безопасности США (АНБ), которое ранее специализировалось на радиоэлектронном шпионаже, начало сотрудничать с банками с Уолл Стрит, обмениваясь с ними данными о хакерах и предоставляя услуги по защите ИТ-систем последних. Сами же банки в США и Европе неоднократно заявляли, что хакерские атаки, проводимые в их адрес, становятся всё более изощрёнными, а их число неумолимо растёт. До недавнего времени бизнес не слишком охотно сотрудничал с властями, опасаясь, что сотрудничество перерастёт в слежку за собственными клиентами компаний. Ранее ФБР США открыло горячую линию по оповещению банков и промышленных компаний о повышении уровня киберугроз в ответ на те или иные события.

В прессе немало рассказывалось о том, что АНБ располагает большим количеством спутников и станций прослушивания, размещённых во многих странах, которые перехватывают и анализируют не только содержание телефонных переговоров, но и электронной переписки. Организация занимается также расшифровкой секретных кодов и давно уже отвечает за защиту американских правительственных компьютерных сетей от кибератак. По словам директора АНБ, правительство и компании добились определённого прогресса в защите компьютерных сетей, но "по-прежнему сохраняется высокая степень их уязвимости". Он напомнил, что только за последний год успешным атакам со стороны хакеров подверглись такие крупные корпорации, как Google, Lockheed-Martin, а также нью-йоркская электронная биржа Nasdaq. Кстати, ещё год назад независимые эксперты представили исследование, описывающее уязвимость в службе голосовой связи Skype, которая позволяет хакерам с лёгкостью вычислять IP-адреса и прочие данные пользователей.

Что же касается кибервойны, которую ведут США, то 22 мая 2012 г. Комитет по разведке Сената США проголосовал за продление действия поправки к закону FISA (её срок истекает в конце 2012 г.), который позволяет перехватывать электронные письма и звонки американцев за рубеж без судебного ордера в целях предотвращения террористических атак. Поправка, одобренная ещё администрацией Буша после терактов 11 сентября, позволяет контролировать электронные коммуникации без специального ордера на каждое лицо, поставленное на прослушку, если лицо не является американцем и находится за пределами США. В результате генеральный прокурор и директор национальной разведки могут получать у судьи ордер на массовые прослушки неограниченного числа лиц. Кроме того, ФБР сформировало новое подразделение — National Domestic Communications Assistance Center (NDCAC), — которому поставлена задача разработать новые технологии слежки, включая слежку в Интернете, перехват беспроводной связи и интернет-телефонии, в том числе Skype. Новая структура базируется в Куантико и состоит как из агентов ФБР, так и Службы маршалов США (подразделение Минюста), а также агентства по борьбе с наркотиками DEA. Издание напоминает, что Куантико уже несколько лет является аналогом Силиконовой долины в области технологий слежки.

Ну а раз уж преступником может стать каждый, то ФБР США внедряет новую систему распознавания на основе биометрической информации, которая идёт на смену морально устаревшей общенациональной базе данных с отпечатками пальцев. Система, получившая название NGI (Next Generation Identification, "идентификация нового поколения"), будет содержать отпечатки пальцев, фотографии радужной оболочки глаз, фотоснимки лиц, образцы ДНК, образцы голоса и другие биометрические данные. Её разработка стоила около 1 млрд долл. Единая база данных позволит гораздо быстрее определить личность правонарушителей и проводить оперативно-розыскные мероприятия по горячим следам. NGI работает с февраля 2012 г. в тестовом режиме в пяти штатах США, а к 2014 г. она будет внедрена по всей территории страны. Учёные, разрабатывающие алгоритмы опознания, утверждают, что их система способна определить нужного человека, даже если он не смотрит прямо в камеру наблюдения. Программа, используя имеющиеся в базе данных фотографии, строит 3D-модель головы объекта поиска и с её помощью способна отыскать подозреваемого, если он прячется за очками или отрастил бороду и усы. Программа способна использовать материалы, отснятые инфракрасной камерой, и находить преступников даже в тёмных переулках. ФБР не гарантирует, что будет включать в базу данных только информацию о преступниках. Данный факт вызывает у граждан США особенное возмущение. Правозащитники опасаются, что в систему можно закачать копии удостоверений личности, образцы ДНК из медицинских баз данных, а также фотографии радужных оболочек глаз, хранящиеся в базах коммерческих компаний — и тогда у ФБР окажется слишком мощный инструмент для слежки за гражданами и подавления демократических свобод.

Что касается успешных кибероперации, то в июне стало известно о завершении масштабной международной операции, в результате которой в 13 странах были арестованы 24 хакера, обвиняемые в торговле похищенными данными кредитных карт и другой финансовой информацией. В совместном заявлении ФБР и прокуратуры Нью-Йорка говорится, что 11 подозреваемых в мошенничестве были арестованы в США, шестеро — в Великобритании, двое — в Боснии и Герцеговине, по одному — в Болгарии, Норвегии, Италии, Японии и Германии. Расследованием этого дела занимались также правоохранительные органы Австралии, Канады, Дании и Македонии. Обезвредить хакеров удалось благодаря подставной операции, которую в течение двух лет проводило ФБР. В июне 2010 г. агенты создали интернет-форум Carder Profit, на котором зарегистрированные пользователи могли продавать и покупать похищенные

тел. 608-83-05
Приём статей: mail@radio.ru
Вопросы: consult@radio.ru
РАДИО № 1, 2013

данные кредитных карт и другую банковскую информацию. Властям удалось собрать доказательства противозаконной деятельности участников форума и предъявить им обвинения. В мае 2012 г. форум был закрыт, а с его постоянными клиентами стали конкретно разбираться. Согласно информации властей США, подставной сайт помог им спасти от хищения 205 млн долл., принадлежащих более чем 410 тысячам владельцам кредитных и дебетовых карт по всему миру.

Газета Washington Post недавно сообщила о том, что "продвинутый" компьютерный вирус под названием Flame, который собирал разведданные и готовился для проведения кибератак, направленных на замедление кампании Ирана по созданию собственного ядерного оружия, совместно разработан по заказу властей США и Израиля. Программа Flame, о которой эксперты российской "Лаборатории Касперского" говорят, как о "возможно, самом сложном вирусе в истории", а в прессе называют "самым опасным кибероружием", собирала данные о местоположении иранских правительственных компьютерных сетей, а также занималась мониторингом активности в них, отсылая своим создателям массивные потоки секретных материалов в рамках подготовки к масштабным кибератакам против Ирана. Как поведала Washington Post, в данной инициативе активно участвовали АНБ США, ЦРУ и израильские военные, а при создании Flame специалисты этих организаций использовали образцы различных опасных деструктивных программ, таких как вирус Stuxnet, которые должны были вызывать различные неполадки в иранском оборудовании, использовавшемся для обогащения урана.

В целом же речь идёт о подготовке поля боя для тайных операций другого типа. Вирусы Flame и Stuxnet являются одними элементами более масштабной атаки, которая всё ещё продолжается сегодня. Вирус Flame был обнаружен экспертами "Лаборатории Касперского" в мае 2012 г. в ходе расследования, инициированного "Международным Союзом Электросвязи" (ITU). Программа-шпион была найдена в ряде стран, преимущественно относящихся к ближневосточному региону. Flame состоит из пакета модулей, который, будучи полностью развёрнутым, занимает около 20 МБ. В этой связи он является трудно поддающейся анализу вредоносной программой. Большой размер вирусу придают множество включённых в него библиотек, например, для сжатия (ZLib, libbz2, PPMD) и работы с базами данных (sqlite3). Кроме того, Flame включает в себя виртуальную машину LUA. После своего внедрения в систему Flame способен проводить комплекс действий, например, перехват сетевого трафика, снятие скриншотов, запись аудиоразговоров, перехват клавиатуры и т. п. Все похищенные данные доступны для операторов трояна через командные серверы. На первый взгляд, Flame не имел ничего общего с исследованными ранее образцами Stuxnet и Duqu. Однако результаты последнего исследования доказывают, что разработчики платформ Tilded и Flame сотрудничали, а Stuxnet содержит в своём ресурсе компонент на платформе Flame. В отличие от Duqu и Stuxnet, Flame атакует не только компьютеры энергетической промышленности, но и ПК конечных пользователей, госучреждений и образовательных организаций.

В августе Агентство передовых оборонных исследовательских проектов (DARPA) при Министерстве обороны США запустило программу под кодовым названием Plan X. Согласно официальному документу, размещённому в Интернете, целью Plan X является "создание революционных технологий, которые позволят понимать, планировать и управлять кибервойной в режиме реального времени, в крупных масштабах, в динамичных сетевых инфраструктурах". Целью Plan X, согласно документу, также является "проведение инновационных исследований для того, чтобы разобраться в сути кибервойн и разработать фундаментальные стратегии и тактику, необходимые для доминирования на поле битвы в киберпространстве". Программа разделена на четыре ключевые области: разработка технологий автоматического анализа для планирования кибероперации (в частности, анализа топологии сетей и сетевых узлов), разработка технологий для автоматического управления операциями с возможностью контроля, разработка операционных систем и платформ для анализа повреждений, развёртывания боевых технологий и адаптивной защиты и разработка технологий визуализации поля кибервойны.

Что касается России, то она, по мнению некоторых американцев, является более серьёзной киберугрозой, чем Китай. В частности, так утверждал в августовском выпуске электронного журнала Defence Dossier, издаваемого Американским советом по внешней политике, Дэвид Смит, директор некоммерческой организации Potomac Institute Cyber Center, занимающейся вопросами кибербезопасности. Россия имеет широкую концепцию информационной войны, включающую в себя разведывательную и контрразведывательную работу, дезинформацию, электронные войны, ослабление связей, нарушение поддержки навигации, психологическое давление и разрушение информационных систем. Впрочем, господин Смит много чего ещё наговорил, но, скажите, что же он мог ожидать, если идёт война всех против всех?

Недавно Уильям Бинни, бывший технический директор АНБ, обвинил нынешнего директора генерала Кита Александера в обмане во время выступления последнего на конференции Defcon 2012 в Лас-Вегасе. Мол, АНБ не занимается сбором данных на рядовых американцев. Бинни говорит, что АНБ начало активно собирать данные и шпионить за американцами после терактов 11 сентября 2001 г. Косвенно это подтверждается исками к АНБ операторов Quest, AT&T и Verizon в 2007 г. Независимые юристы говорят, что формально АНБ не имеет конституционных прав вести негласную слежку за жителями страны, но в последние полтора десятка лет было принято столько поправок, что фактически ведомство может найти юридические обоснования для национального шпионажа.

В ноябре каждого года в течение нескольких последних лет проводятся военные учения НАТО "Cyber Coalition". Они посвящены отработке совместных действий стран-участниц Альянса в условиях кибервойны. В 2012 г. в качестве условного агрессора — некая "африканская страна", хотя на деле американские военные признаются журналистам, что главными киберагрессорами считается, скорее, Россия или Китай.

Что ожидать дальше? Разве что распространения всего приведённого опыта на все вовлечённые в кибервойну страны. Впрочем, это вполне логичная расплата за Интернет, если в моральном плане население планеты всё ещё находится на уровне дикарей.