InformationSecurity
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

В рубрику "Кибервойна" | К списку рубрик | К списку авторов | К списку публикаций

Кибервойны будущего – к чему готовиться законодателям и корпорациям

Термин “кибервойна" мы связываем с термином “кибернетика" (“наука об управлении", “управление и связь с животным и машиной" – по Н. Винеру, 1948 г.), а также с понятием “цифра" (обратите внимание на написание слов “cyber" и устаревшего – “цифирь", еще петровского времени). Поэтому нужно смотреть на проблему кибервойн более широко, чем это принято. Что это значит? Классическая война – это “горячая война" с использованием материального оружия и энергии, которая до поры до времени упрятана в материи (атомное оружие и т.п.). Действующими компонентами такой войны являются материя и освобожденная из нее энергия.

Игорь Башелханов
Заведующий лабораторией, преподаватель,
ФГОБУ ВПО Финансовый университет при Правительстве Российской Федерации, к.ф.-м.н.

Кибервойна – это массированная обезличенная генерация хаоса в социотехнической системе, связанная с совместным применением программируемых технических средств и программируемых социальных элементов (биоисполнителей, биороботов). Программа (последовательность команд) – это идеальное оружие (прежде всего, в философском смысле – вспомним материалистическое и идеалистическое течения в философии). Это оружие идеально и в обычном смысле: на первых порах оно не приводит к летальным последствиям для людей, оно невидимо, не оставляет материальных следов, а если следы и остались – легко уничтожаются. Рука об руку с программированием идут математика и информационная безопасность (где цифра – там и математика, а за ней видна криптография). На данном этапе развития технологий можно говорить о гибридном социотехническом оружии. Речь идет об использовании в кибервойне не только ИКТ, но и исполнителей – людей (так называемых "животных", по терминологии "отца кибернетики") – и исполнительных устройств – машин. Промежуточной целью любых войн является создание хаоса (разрушение старых связей и отношений, в особенности – образовательных, политических, экономических), которое дает возможность в конечном счете переключить источники энергии-информации пораженной социотехнической системы на нового бенефициара, выгодоприобретателя. Финансово-экономическими признаками начала кибервойны можно назвать замедление роста, остановку, а затем падение валового внутреннего продукта (ВВП) страны-жертвы условно более чем на один процент за один месяц.

> Первая мировая война была, образно говоря, войной прикладных химиков, Вторая мировая война – войной прикладных физиков, третья мировая война станет войной математических физиков и прикладных математиков.

Теория динамического хаоса

Кибервойна – это массированная обезличенная

Теории хаоса, точнее, динамического хаоса, были развиты французским

> генерация хаоса в социотехнической системе, связанная с совместным применением программируемых технических средств и программируемых социальных элементов (биоисполнителей, биороботов). Программа (последовательность команд) – это идеальное оружие

физиком, философом Анри Пуанкаре, советскими математиками-академиками А.Н. Колмогоровым, В.И. Арнольдом и немецким математиком Ю.К. Мозером (КАМ-теория). Приложил свой ум к его развитию и физикохимик русского происхождения Илья Пригожин – нобелевский лауреат, автор "Философии нестабильности". Американскими химиком Джорджем Коуэном и физиком Мюрреем Гелл-Манном был создан в 1984 г. Институт сложности в Санта-Фе (SFI). В дальнейшем над этими проблемами работали советский и российский академик А.А. Самарский, член-корреспондент РАН С.П. Курдюмов и продолжает работать профессор Г.Г. Малинецкий и их партнеры. Поскольку вышеперечисленные ученые знали механизмы зарождения и эволюции хаоса, то они могли предложить "противоядие", "противооружие". Наиболее четко видевшим гуманитарные проблемы, проистекающие из реалий и планов математической войны, был академик В.И. Арнольд [1]. Приведем цитату из речи В.И. Арнольда на парламентских слушаниях 2002 г., эмоционально изображающую план поражения в этой войне: "Этот план производит общее впечатление плана подготовки рабов, обслуживающих сырьевой придаток господствующих хозяев: этих рабов учат разве что основам языка хозяев, чтобы они могли понимать приказы". Вот другие слова, приписываемые Арнольду: "Вот почему бурбакистская мафия, заменяющая понимание науки формальными манипуляциями с непонятными "коммутативными" объектами, так сильна во Франции, и вот что угрожает и нам в России". Разъясняя это, математик приводит пример: "Французский школьник-отличник на вопрос: "Сколько будет два плюс три?" отвечает: "Три плюс два, так как сложение коммутативно", а считать до пяти, хотя бы на пальцах, его не научили (видимо, вследствие "компьютерной дидактики")". "Физико-математический абсолют" и злоумышленники создают так называемый "управляемый хаос" во всех сферах жизни поражаемого общества, зачастую интуитивно (невольно, подсознательно) используя теорию динамического хаоса.

Математические войны

Поскольку войны могут длиться десятилетиями, для "физико-математического абсолюта" или для злоумышленных выгодоприобретателей очевидно, что наиболее эффективным способом является математическое, программное поражение детей и молодежи. Через такую математико-"артиллерийскую" подготовку первоначально прошли французские и американские молодые люди, а затем европейские и украинские учащиеся и студенты. Понятие о "математических войнах" появилось в США в конце 80-х – начале 90-х гг. XX в. и отражает уровень накала страстей по проблемам школьной математики. В Европе подобные войны коррелируют с "болонским процессом". Начало "математико-цифровым войнам" положила публикация в 1989 г. нового стандарта школьного математического образования, подготовленного Национальным советом учителей математики США (National Council of Teachers of Mathematics, NCTM). Результатом почти двадцатилетних математических войн стал мировой кризис 2008 г., наступивший из-за деградации и хаоса в головах американской и европейской молодежи, а также молодежи других частей планеты, которая в свое время вольно или невольно клюнула на программную удочку и которая за это время стала элитой политики, бизнеса и других сфер.

Будущая "идеальная кибервойна" будет включать не только применение нормативно-право-конституционных, организационно-экономико-маркетинговых методов поражения противника, но и применение непосредственно физико-технико-математического оружия, но уже в полном объеме.

Заключение

Квантовый компьютер, устроенный на физических принципах квантовой механики, легко может взломать шифр RSA, алгоритм DES, стандарт RC5 и т.п., и,

Будущая "идеальная кибервойна" будет включать не только применение нормативно-право-конституционных (НПК), организационно-экономико-маркетинговых методов (ОЭМ)

таким образом, самая секретная и конфиденциальная информация, возможно, уже завтра станет явной – тайна исчезнет.

поражения противника, но и применение непосредственно физико-технико-математического оружия (ФТМ), но уже в полном объеме [2]. Первые две группы мер также уже сейчас имеют явные или неявные математические признаки. В настоящее время "обкатывается" часть элементов этой войны в виде взаимных экономико-политических санкций – самоотказов в обслуживании (DoS и DDoS-самоатаковывание) – ущербное не только для технических, но и для социальных подсистем. Вспомним также использование термина "перезагрузка" президентом США Б. Обамой. Таким образом, компьютерный подход распространяется на социально-государственные отношения. Соответственно, НПК (оружию должны противопоставляться НПК) – меры защиты. Нормативы – это стандарты, инструкции, политики безопасности. Для того, чтобы отсечь "раковые опухоли", последствия перерождения собственных элементов, инсайдеров (перепрограммирования нейронных клеток и в целом людей) во время будущей кибервойны, нужно установить собственные стандарты, нормативы, политики безопасности, нужно создавать, сохранять и развивать свои языки, в том числе и языки программирования, создавать свои операционные системы и т.п., не распространяя их по всему миру, поскольку при их совместимости очень вероятными становятся вирусные пандемии (как в случае, например, с вирусом Эбола), но уже в виртуальном пространстве. Аутентичные, этнические, национальные стандарты должны быть обязательны для исполнения. В правовом поле, регулирующем ИКТ и информационное право, органам нужно устанавливать цифровое правосудие, работающее уже в наносекундном режиме и во всем цифровом пространстве. Поэтому на международном уровне должен быть введен Цифровой кодекс. Нужно устанавливать пределы гонки цифровых вооружений путем заключения международных договоров.

Корпорациям, во-первых, важно иметь в виду, что качество и количество DoS- и DDoS-атак и других инцидентов информационной безопасности подчиняется математическим закономерностям, а также что они определяются на 70–80% непосредственно уязвимостями человека, человеческим фактором. Во-вторых, с маркетинговой точки зрения нужно срочно обратить внимание на способность их цифро-программных устройств различного назначения обеспечивать информационную безопасность. В-третьих, производителям и потребителям надо знать, что в 2006 г. исследовательская группа из Лос-Аламосской национальной лаборатории (США) впервые произвела передачу секретной информации на расстояние больше чем 100 км, используя принцип квантовой криптографии, теоретически обеспечивающей абсолютную тайну переданного сообщения. Дальнейшее, уже засекреченное, развитие этой отрасли приведет к бессмысленности DLP, BYOD, к краху и смерти классической математической криптографии и современных программно-аппаратных средств защиты информации. Квантовый компьютер, устроенный на физических принципах квантовой механики, легко может взломать шифр RSA, алгоритм DES, стандарт RC5 и т.п., и, таким образом, самая секретная и конфиденциальная информация, возможно, уже завтра станет явной – тайна исчезнет.

Литература

1. Арнольд В.И. Что такое математика? – М.: МНЦМО, 2012. – 108 с.

2. Башелханов И.В., Башелханов С.И. Концепция защиты информации. Новые аспекты обеспечения информационной безопасности // VI Международная научно-практическая конференция студентов, аспирантов и молодых ученых "Информационные технологии в науке, бизнесе и образовании (Технологии безопасности)". – М.: Изд-во Финуниверситета. – 2013. – С. 35–38

Опубликовано: Журнал "Information Security/ Информационная безопасность" #5, 2014

Статьи про теме