per Concordiam

Журнал по проблемам безопасности и обороны Европы

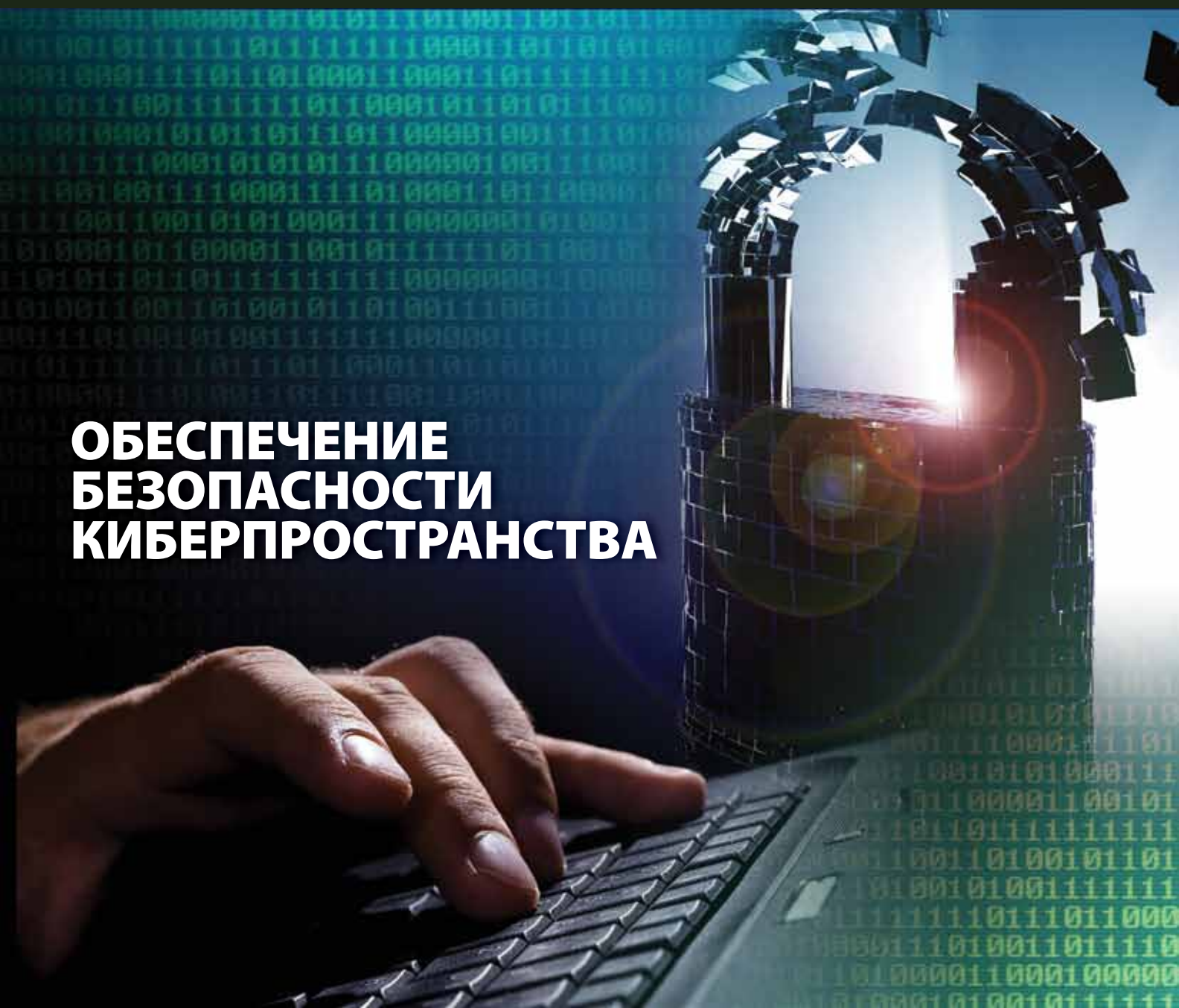
■ **ДИАГНОЗ ПРОБЛЕМЫ**
Обнаружение источников кибератак

■ **НЕЖЕЛАТЕЛЬНЫЕ ТЕНДЕНЦИИ**
Хакеры обходят закон

■ **КИБЕРНЕТИЧЕСКИЙ АЛЬЯНС**
Бизнес устанавливает партнерские отношения с правительством

■ **КАВКАЗ РАЗВИВАЕТ ТУРИЗМ**
Возрождение туризма приносит прибыль

ПЛЮС
Интеграция европейских рома
В защиту афганских женщин
В поисках «чистого электричества»



ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КИБЕРПРОСТРАНСТВА

Содержание

основные статьи

НА ОБЛОЖКЕ

Отражение нападений на жизненно важные компьютерные сети, как военные, так и гражданские, стало главной целью Европейского оборонительного сообщества. Скрываясь среди более миллиарда веб-пользователей и десятков миллионов веб-сайтов, киберпреступники научились мастерски использовать компьютеры как дешевое анонимное оружие, часто оставаясь при этом безнаказанными. НАТО и Европейский Союз делают успехи в выявлении и наказании хакеров, представляющих угрозу безопасности.

ИЛЛЮСТРАЦИЯ *PER CONCORDIAM*

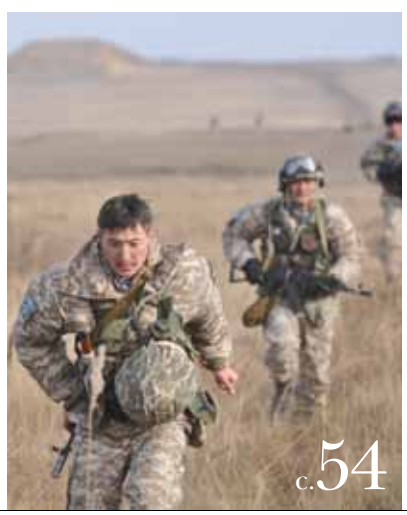
разделы


с.22

СОТРУДНИЧЕСТВО

БЕЗОПАСНОСТЬ

ПОЛИТИКА


с.54


с.60

GEORGE C. MARSHALL
EUROPEAN CENTER FOR SECURITY STUDIES

Добро пожаловать

на страницы шестого номера журнала *per Concordiam*, в котором мы раскрываем тему кибербезопасности. Чем крепче компьютерные сети связывают мир воедино, чем больше государства полагаются на компьютерные технологии и высокоскоростные средства связи, тем сильнее растут угрозы неприкосновенности частной жизни наших граждан, целостности наших деловых операций, безопасности наших объектов критической инфраструктуры и даже боеготовности наших вооруженных сил. Такие традиционные меры обеспечения безопасности, как географические расстояния или наличие регулярной армии, способной обеспечить устрашение сравнимых по силе противников или победу над ними, плохо работают против тех, кто готов воспользоваться кибернетическим пространством для несанкционированных, враждебных или незаконных действий.

Кибернетические угрозы могут носить самый разнообразный характер: от подросткового вандализма до поддерживаемого государством шпионажа, от традиционной организованной преступности до злонамеренного воздействия на отдельных индивидов, от подстрекательства к бунту (как на начальных стадиях кибернетической атаки на Эстонию в 2007 году) до тайного размещения оружия, которое будет использовано в случае войны между странами. Из этих примеров видно, что разнообразие кибернетических атак ограничено скорее воображением агрессора, чем способностью обороняющегося выявлять и предотвращать подобные атаки.

На пути эффективной и законной кибернетической обороны стоит множество препятствий. Сетевые технологии значительно упрощают проведение анонимных операций и даже операций под чужим флагом. Высокая скорость, с которой протекают кибернетические операции, практически не оставляет времени на такие меры, как эффективное расследование проникновений, консультативное сотрудничество между странами-жертвами атаки или правовая экспертиза возможных ответных действий, а также возникновение необходимости в немедленных защитных действиях. Законодательство, регулирующее проведение кибернетических операций, охватывает весь диапазон от вопросов правоприменения внутреннего уголовного законодательства до судебных решений в области международного права, относящихся к «применению силы» и «вооруженному нападению», дающих право на на самооборону. И, наконец, государственной политике в области кибернетической безопасности мешают трудности межведомственного сотрудничества, а также то, что подавляющее большинство целей потенциальных кибернетических атак находятся в частном секторе экономики, за пределами области непосредственного контроля большинства правительств.

Для предотвращения потенциальных кибернетических угроз лидерам европейских и евразийских государств следует использовать общенациональный подход для реализации программ защиты объектов критической инфраструктуры, стимулирующих взаимодействие между правительством и ключевыми компаниями частного сектора.

Несмотря на вполне реальные угрозы, описанные выше, развитие информационных технологий будет продолжать ускоряться. Эти технологии предоставляют большие преимущества, такие как экономическая эффективность, политическая прозрачность и глобальная интеграция. Поэтому необходимо, чтобы эксперты в области безопасности предложили анализ и рекомендации, которые позволили бы реагировать на эти угрозы и справляться с ними. В решение этой задачи призваны внести свой вклад как данный номер журнала *per Concordiam*, так и исследовательские, образовательные и информационно-разъяснительные программы Центра им. Дж. Маршалла.

Мы приветствуем ваши мнения и комментарии по вопросам кибербезопасности. Ваши комментарии будут опубликованы в двух следующих выпусках журнала *per Concordiam*, которые будут посвящены, соответственно, международному праву и будущему Афганистана. Пожалуйста, пишите нам по адресу editor@perconcordiam.org.

Искренне ваш,

Кит В. Дейтон
Директор

Кит В. Дейтон
Директор
Центр им. Дж. Маршалла

Кит Дейтон вышел в отставку с военной службы в Армии США в конце 2010 г. в звании генерал-лейтенанта, прослужив в вооруженных силах более 40 лет. Его последним назначением на действительной военной службе была должность Координатора США по вопросам безопасности между Израилем и Палестиной в Иерусалиме. В его послужном списке служба в качестве офицера-артиллериста, а также работа на посту офицера по военно-политическим вопросам при штабе Сухопутных войск США в Вашингтоне (округ Колумбия) и военного атташе США в Российской Федерации. В его послужном списке работа на посту директора аналитической группы по Ираку в ходе операции «Иракская свобода». Генерал-лейтенант Дейтон проходил стажировку в Колледже для старшего руководящего состава при Гарвардском университете. Он также являлся старшим стипендиатом от Армии США в Совете по международным отношениям в Нью-Йорке. Генерал-лейтенант Дейтон имеет степень бакалавра истории от Колледжа Вильгельма и Марии, степень магистра истории от Кембриджского университета, а также степень магистра международных отношений от Южнокалифорнийского университета.

Витаутас Бутримас – работает в сфере информационных технологий и коммуникаций более 20 лет, начав свою карьеру с должности компьютерного специалиста в округе Принс-Уильям (штат Виргиния, США) и поднявшись до поста заместителя министра Министерства коммуникаций и информатики Литовской Республики. В 1998 году он поступил на службу в Министерство обороны в качестве директора по разработке руководящих принципов и планированию. С 2001 года г-н Бутримас работает заместителем директора Центра безопасности информационных систем, находящегося в ведении Министерства обороны. В 2009 году он являлся руководителем целевой группы, подготовившей план стратегии и внедрения кибероборонны. Г-н Бутримас является выпускником семинара для высшего руководящего состава Центра им. Дж. Маршалла.

Д-р Вячеслав Дзюндзюк – профессор Харьковского регионального института Национальной Академии Государственного управления. Специализируется на современных политических и геополитических процессах, проблемах информационной безопасности и правительственных реформ. Профессор Дзюндзюк является автором монографии и многочисленных статей, а также соавтором нескольких книг, посвященных этим вопросам. Имеет докторскую степень по вопросам государственного управления и является выпускником программы углубленного изучения вопросов безопасности Центра им. Джорджа Маршалла 2008 года.

Александр Климбург – научный сотрудник Австрийского института иностранных дел. С 2006 г. г-н Климбург ведет работу по проектам национальной правительственной безопасности Федеральной Канцелярии Австрии при Министерстве обороны и Совете национальной безопасности. Он предоставляет консультации различным национальным правительствам и государственным учреждениям и является главным автором проводимого под эгидой Европарламента исследования по вопросам кибервойны. Его работа в сфере кибербезопасности прежде всего касается вопросов информационной безопасности, защиты стратегической информационной инфраструктуры и понятий кибервойны, кибертерроризма и киберпреступности. Он является автором рекомендательных документов, а также одним из соавторов книги «Inside Cyber Warfare». Ему присуждены ученые степени Лондонской школы исследования стран Востока и Африки и Лондонской школы экономики..

П-к Ильмар Тамм – директор Передового Центра Сотрудничества НАТО по Вопросам Кибероборонны в Эстонии. П-к Тамм – выпускник Финской военной академии 1994 года; был офицером связи и прошел обучение в качестве штабного офицера в Эстонском колледже национальной обороны. Служил в Генеральном штабе эстонских оборонительных сил начальником отдела коммуникаций и информационных систем. Затем п-к Тамм был назначен на службу в Генеральный штаб объединенного командования сухопутных войск в г. Гейдельберге и направлен в Афганистан, где работал в Генштабе Международных сил содействия безопасности начальником операций объединенного Центра контроля над информационными системами и коммуникациями. П-к Тамм награжден, помимо прочих наград, крестом «За выдающиеся заслуги» эстонских сил обороны и медалью НАТО «За безупречную службу».

Новак Джорджиевич – офицер ВВС Сербии, пилот истребительной эскадрильи. Ранее работал в Центре воздушных операций и имеет большой опыт в вопросах военно-воздушных операций и военно-гражданского воздушного движения. Является выпускником программы углубленного изучения вопросов безопасности Центра им. Джорджа Маршалла, а также имеет степень магистра по информационным системам Белградского университета. В настоящее время работает над докторской диссертацией. Опубликовал две книги об авиации и разработал Интернет-сайт, посвященный авиации, научным вопросам и информационным технологиям.

Кеннет Гирс – (Доктор Философии, Сертифицированный Специалист НАТО по безопасности Информационных Систем), Военно-Морская Служба Уголовных Расследований), – ученый и представитель США в Передовом Центре Сотрудничества по Вопросам Кибероборонны (CCD CoE) в г. Таллинне (Эстония). Г-н Гирс служил разведаналитиком, специалистом-лингвистом по французскому и русскому языкам и компьютерным программистом в поддержку инициативы контроля над стратегическими вооружениями.

Д-р Брет Майкл – преподаватель информатики и электротехники в Школе повышения квалификации личного состава ВМС. Ранее занимал различные исследовательские должности в Университете Калифорнии в Беркли, Национальной лаборатории в Аргонне и Институте военных исследований. Будучи специалистом по распределенным системам и системам с гарантированной безопасностью, который также интересуется правом и принципами управления, он служит техническим советником для группы экспертов, разрабатывающей «Таллиннское Руководство по Международному Праву Применительно к Киберконфликтам». В течение трех лет работал ответственным редактором журнала «IEEE Security & Privacy». Является доктором информационных технологий Университета Джорджа Мейсона (штат Виргиния, США).

Профессор Томас Вингфилд – преподаватель международного права в Центре им. Дж. Маршалла. В 2009 и 2010 гг. служил советником по вопросам гражданского правопорядка Консультативной группы по борьбе с повстанческим движением в составе МССБ в Афганистане. Бывший офицер ВМС; работал в частном секторе, научно-исследовательских институтах и научных сообществах, включая Командно-штабной колледж СВ США. Г-н Вингфилд – бывший председатель Комитета по вопросам международного уголовного права Американской ассоциации адвокатов и автор работы «The Law of Information Conflict: National Security Law in Cyberspace». Доктор и магистр международного и сравнительного права Юридического центра Джорджтаунского университета в Вашингтоне.

per Concordiam

Журнал по проблемам безопасности и обороны Европы

Кибербезопасность

Том 2, Выпуск 2

Центр имени Маршалла

Персонал этого, открытого в 1993 году, института призван воплощать в XXI веке видение разработанного после Второй мировой войны Плана Маршалла. Центр способствует развитию диалога и взаимопонимания между народами Европы, Евразии, Северной Америки и других регионов мира. Общая идея всех программ очного обучения и мероприятий по взаимодействию: большая часть проблем безопасности в XXI веке требует международного, межведомственного и междисциплинарного реагирования и взаимодействия.

Контактная информация:
Per Concordiam editors
George C. Marshall Center
Gernackerstrasse 2
82467 Garmisch-Partenkirchen
Germany
http://tinyurl.com/per-concordiam-magazine

Наша жизнь во многом зависит от компьютеров и Интернета. Люди пользуются компьютерами в самых разнообразных целях – от переписки по электронной почте, общения в чатах и обмена фотографиями до ведения банковских дел, осуществления инвестиций, совершения покупок и планирования отпуска. Правительства, вооруженные силы, деловые круги и организации национальной безопасности также зависят от компьютерных сетей. Эта зависимость от Интернета спровоцировала целое множество угроз в киберпространстве. Данный выпуск «*per Concordiam*» посвящен растущему беспокойству стран Европы и Евразии в отношении кибертерроризма, киберпреступности и кибератак, совершаемых неизвестными нарушителями или хакерами, нападающими на стратегически важные компьютерные сети и программы с помощью «зловредного ПО», «червей», троянских вирусов, ботнетов и компьютеров-зомби.

Шестой выпуск «*per Concordiam*» представляет мнение по данному вопросу директор Передового Центра Сотрудничества НАТО по Вопросам Кибероборонь в Эстонии п-ка Ильмара Тамма. В своей статье п-к Тамм подчеркивает потребность в национальных и международных силах и средствах для противостояния росту киберпреступности и кибератак. Он доказывает, что пришло время изменить наше представление о коллективной безопасности и включить киберпространство в число приоритетных вопросов национальной безопасности.

Первый очерк выпуска – «Тревожная тенденция» - дает сбалансированную оценку вопросам кибербезопасности, стоящим перед миром в настоящее время. Витаутас Бутримас, заместитель директора Центра безопасности информационных систем при Министерстве Литвы и дважды выпускник Центра им. Дж. Маршалла, описывает последние кибератаки и объясняет ценность обмена информацией при попытках выявления источника атаки.

Следующая статья – «Остановить кибертерроризм» - написана профессором Харьковского регионального института Национальной академии государственного управления (Украина) д-ром Вячеславом Дзюндзюком, выпускником программы углубленного изучения вопросов безопасности Центра им. Джорджа Маршалла 2008 года. Всего 20 лет тому назад приставка «кибер-» использовалась лишь в фантастической литературе. С тех пор, однако, такие слова, как «киберпространство» и «кибертерроризм» прочно вошли в современный лексикон. К сожалению, то же самое можно сказать и о кибертерроризме. Для борьбы с этой новой формой терроризма требуются новые подходы и методы. Д-р Дзюндзюк говорит об эволюции киберпреступности в целом и о кибертерроризме в частности, а также перечисляет возможные способы противодействия им.

Мировое руководство озабочено тем, что кибертерроризм и кибервойна могут стать серьезной угрозой национальной безопасности. К сожалению, кибератаки и кибероборона часто остаются тайной для тех, кому не хватает знаний в области информационных технологий и вычислительной техники. Кеннет Гирс – представитель США в Передовом Центре Сотрудничества НАТО по Вопросам Кибероборонь в Эстонии – дает ясные технические пояснения простым языком в своей статье «Предотвращение хакерских атак». В своей работе автор в доступной форме говорит о понятии киберугрозы, сузив его до базовых концепций и определений с целью оказания помощи стратегам, работающим в области кибероборонь.

В статье «Сила в единстве» автор Александр Климбург из Австрийского института международных дел использует общегосударственный подход для объяснения извлеченных им уроков в сфере кибербезопасности. Четыре приведенных примера иллюстрируют задачи и сложности, стоящие перед правительствами в отношении обеспечения защиты объектов жизнеобеспечения посредством сотрудничества с ключевыми компаниями частного сектора. Г-н Климбург приходит к выводу, что государствам необходимо содействовать межорганизационному сотрудничеству, включая неправительственные структуры.

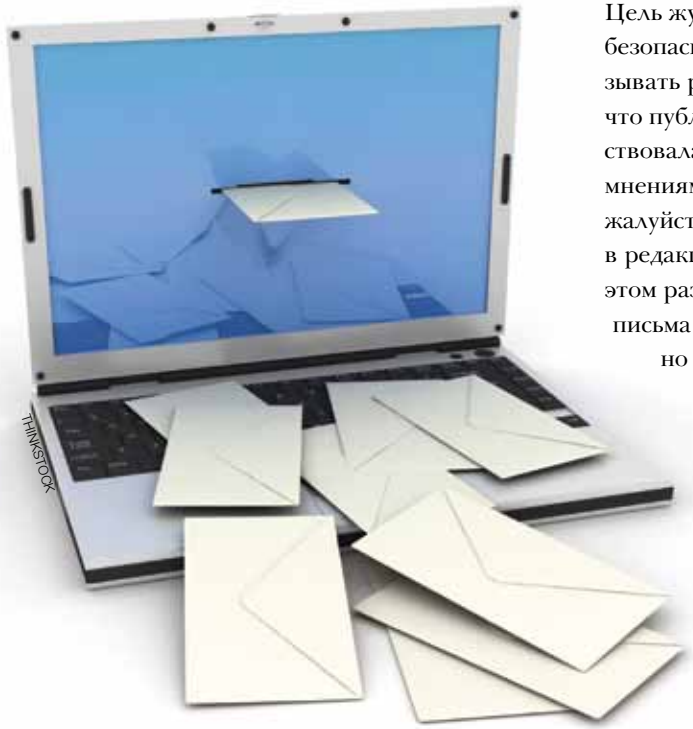
«Как защитить кибернетическое пространство» - статья, написанная Новаком Джорджиевичем, летчиком-истребителем сербских ВВС и выпускником Центра им. Дж. Маршалла, - доказывает, что существующая защита компьютерных сетей слишком полагается на оборонительный подход и реагирование. Слишком поздно действовать, когда нападение уже совершено. Он объясняет, что риски киберпреступников малы, а выгода огромна, и призывает международное сообщество разработать системный подход для прекращения того, что он считает организованной преступностью.

Последняя авторская статья – «Новая эра ответственности» - написана д-ром Бретом Майклом, преподавателем информатики и электротехники в Школе повышения квалификации личного состава ВМС США, и д-ром Томасом Вингфилдом, преподавателем международного права в Центре им. Дж. Маршалла. Авторы описывают внутренние и международные проблемы и задачи реагирования на преступления и терроризм в киберпространстве. В их статье показывается, как анонимность, шифровка данных и коммуникационные платформы усложняют установление источника преступления в киберпространстве; авторы призывают к принятию решений, учитывающих политические, правовые и технологически вопросы.

В следующем выпуске «*per Concordiam*» будет рассматриваться новая стратегическая концепция НАТО, а затем последует выпуск, посвященный изменениям в Северной Африке и на Ближнем Востоке. Мы приглашаем вас и ваших знакомых предложить «*per Concordiam*» статьи по данным темам.

Мы рады Вашим отзывам и ждем электронных писем от вас для продолжения постоянного диалога о важных вопросах безопасности. Каждый наш выпуск доступен в электронном виде в Интернете на сайте Центра им. Джорджа Маршалла:
http://tinyurl.com/per-concordiam-magazine

— редакционная коллегия *per Concordiam*



Цель журнала *per Concordiam* – рассматривать проблемы безопасности, актуальные для Европы и Евразии, и вызывать реакцию читательской аудитории. Мы надеемся, что публикация наших первых пяти номеров способствовала этому и помогла начать обсуждение и обмен мнениями Мы приветствуем ваши отзывы, поэтому, пожалуйста, делитесь с нами своими мыслями, присылайте в редакцию письма, которые мы будем публиковать в этом разделе. Пожалуйста, постарайтесь, чтобы ваши письма были по возможности короткими и обязательно указывайте статью, автора и номер журнала, на которые вы ссылаетесь. Мы оставляем за собой право редактировать все письма с точки зрения языка, стиля, точности, краткости и ясности изложения.

Просим направлять отзывы электронной почтой по адресу editor@perconcordiam.org

Подача материалов для публикации

Цель *per Concordiam* – быть сбалансированным журналом, который будет каждый квартал публиковать наиболее интересные и яркие из поданных на публикацию статей. Мы будем рады статьям от читателей на темы безопасности и обороны в Европе и Евразии.

Сначала направьте нам по электронной почте editor@perconcordiam.org тему своей статьи в виде краткого содержания или описания. Если нам понравится идея, Вы получите ответ еще до того, как начнете писать. Мы принимаем только оригинальные статьи. Если Ваша статья или аналогичный материал рассматриваются для публикации в другом издании или уже были где-то опубликованы, сообщите нам об этом при подаче материала. Если у Вас уже есть рукопись для издания, но Вы не уверены в том, подходит ли она для ежеквартального издания, свяжитесь с нами по электронной почте, чтобы узнать заинтересует ли нас Ваш материал.

Когда Вы пишете статью, пожалуйста, помните:

- **Избегайте очевидного.** Мы ищем статьи с уникальными для региона подходами. Вероятнее всего, мы не опубликуем статьи на темы, которые широко освещаются другими изданиями, публикующими материалы по безопасности и внешней политике.
- **Ищите взаимосвязи.** Мы опубликуем статью об одной стране, если тема статьи актуальна для региона или для всего мира.
- **Не ориентируйтесь на аудиторию в США.** Подавляющее большинство читателей *per Concordiam* находятся в Европе и Евразии. Мы с меньшей вероятностью опубликуем статью, если она предназначена для читателей в США. Наша задача – вызвать открытое обсуждение важных тем, касающихся безопасности и обороны, а не быть всего лишь рупором внешней политики США.
- **Избегайте профессионализмов и узкоспециальных терминов.** Не каждый является специалистом в определенной области. Идеи должны излагаться доступно для как можно более широкой аудитории. Предоставьте оригинальные исследования или отчеты в поддержку Ваших идей. Будьте готовы представить документы. Мы производим фактическую проверку всех публикуемых материалов.
- **Авторские права.** За авторами материалов сохраняются их авторские права. Однако, подача материалов для публикации подразумевает, что автор дает *per Concordiam* право на публикацию работы.
- **Биография/фотография.** При подаче материала, пожалуйста, приложите к нему свою краткую биографию и фото в цифровом формате с разрешением не менее 300 DPI.

После этого отправьте нам свою рукопись в формате Microsoft Word по электронному адресу editor@perconcordiam.org в виде приложения.

Слияние кибер- и национальной безопасности

Военная подготовка должна включать оборону компьютерных сетей

П-к Ильмар Тамм, директор Передового Центра Сотрудничества НАТО по Вопросам Кибероборонs в Эстонии

Эволюция и широкий доступ к информационным технологиям предоставляют новые возможности для манипулирования и удовлетворения нездоровых амбиций. Растет количество политически мотивированных кибернетических инцидентов, направленных против безопасности государств, включая их вооруженные силы. С юридической точки зрения, кибернетическая атака повлечет за собой военное реагирование, в случае если она достигла порога «вооруженного нападения», что эквивалентно идущим через границу танкам, уничтожающим людей и недвижимые объекты. Наши силы обороны в ходе осуществления своей невоенной функции должны сдерживать и в случае необходимости - помогать гражданским властям защищаться от кибератак.

Поскольку инциденты в кибернетическом пространстве уже вышли за грань обычных преступлений, использование определения «кибернетическая» со словом «война» лежит не в плоскости «если», а в плоскости «когда» и «как». Кибернетические атаки угрожают попыткам государства развивать информированное общество. Они часто являют собой угрозу национальной безопасности. Кибернетические нападения зашли на территорию военных действий, и это требует полного внимания наших сил обороны. Эти области находятся под прикрытием инструментов, которые регулярно применяются к целому спектру угроз. Для противодействия новой угрозе нам необходимо научиться использовать имеющийся у нас юридический арсенал, включая Женевские Конвенции, Устав ООН и директивы ЕС об информационном обществе. Нам необходимо понять, как усовершенствовать наши национальные стратегии безопасности, чтобы решить проблемы в кибернетическом пространстве и укрепить компьютерную безопасность как составляющую национальной и глобальной безопасности.

ИЛЛЮСТРАЦИЯ PER CONCORDIAM

Нам необходимо понять, как усовершенствовать наши национальные стратегии безопасности, чтобы решить проблемы в кибернетическом пространстве и укрепить компьютерную безопасность как составляющую национальной и глобальной безопасности.

Чтобы лучше понять суть кибернетического пространства и то, как в него вписываются вооруженные силы, Скотт Борг, директор подразделения по последствиям кибернападений США, объяснил существенную разницу между кибернетической обороной и промышленной обороной. Согласно Боргу, кибернетическая оборона подразумевает борьбу с взаимосвязанными группами, которые часто не имеют четкого отношения к определенному государству. Противостоящая сила потенциально рассосредоточена между различными юрисдикциями во всем мире. Кибернетические защитники должны реагировать повсеместно, используя информационные средства вместо традиционной огневой мощи.

В стратегическом смысле кибернетическая оборона имеет гораздо меньшее отношение к защите географических параметров и к внешним угрозам. Чаще объектами нападений являются внутренние сети, и нападения совершаются изнутри. Военно-промышленный комплекс как объект нападений сменился частной инфраструктурой жизнеобеспечения. Говоря военным языком, все это – незащищенные цели, но ценность их крайне высока. Кибернетические атаки изначально не измеряются количеством ранений, смертей или разрушений. Вместо этого ценность уничтоженной информации определяется ее влиянием на функционирование общества государства, включая его вооруженные силы. Тем не менее, кибернетические атаки, в целом, могут привести к увечьям, смертям и разрушениям.

Более того, Борг заявляет, что мы ушли от эпохи принципов сдерживания к эпохе принципов устойчивости. Я бы сказал, что хорошая оборонная концепция по-прежнему обладает достаточным эффектом сдерживания, и считаю, что, разрабатывая планы ответных действий ВС, необходимо принимать во внимание оба принципа.

Все эти факторы влияют на то, как принимаются решения о достижении и поддержке информационного превосходства – состояния, включающего в себя конфиденциальность, целостность и доступность информации в самом широком смысле. Присутствие различных заинтересованных сторон гарантирует постоянный и повсеместный эффективный контроль над информационной инфраструктурой. Планирование усложняется тем, что личность противника неизвестна, а распознать какую-либо модель или полезную информацию из информационного шума – трудно. Реагирование имеет иное значение в кибернетическом пространстве – только технологии могут противостоять технологиям, однако, принятие решений по-прежнему остается за людьми.

Асимметричные угрозы непредсказуемы и, как правило, направлены на самые слабые звенья цепи. Таким образом, звенья, укрепленные исходя из предыдущего опыта, знаменуют собой только начало усилий в сфере обороны. Соответственно, для обеспечения эффективной кибернетической обороны необходимо всегда быть в курсе относительно уровня настоящей опасности и угрозы, то есть того, что военные называют «общей оперативной картиной», равно как и поддерживать способность определять тенденции на основании опыта и наблюдений. Следовательно, даже с теоретической точки зрения, подготовка обороны против кибернетического нападения является наиболее сложной задачей. Когда вы понимаете, что грядет кибернетическая атака, ваш противник знает, что вы это поняли. Передислокация нападения дается значительно проще, чем передислокация обороны.

Как писал Карл фон Клаузевиц в своей знаменитой книге «*О войне*», во время войны генерала постоянно бомбардируют донесениями, как верными, так и неверными; ошибками, вызванными страхом, халатностью или спешкой; неподчинением в результате верной или неверной интерпретации, злого умысла, истинного или ошибочного чувства долга, лени или истощения; а также происшествиями, которые никто не мог предвидеть. Короче говоря, генерал подвержен бесчисленным информационным стимулам, большинство из которых пугающего характера, и лишь немногие - ободряющего. В кибернетическом конфликте задача генерала отягощается тем фактом, что нападения легко осуществить, оборона обходится дороже нападения, а государства часто предпочитают игнорировать киберпреступников или даже поддерживать их на своей территории. Наша жизнь такова, что мы все больше и больше становимся уязвимы к этим нападениям без огня и стрельбы. Пришло время изменить наше мышление и начать интегрировать кибернетическое пространство в нашу картину национальной безопасности, объединив его с развитием оборонного потенциала. □

Тревожная Тенденция

КИБЕРАТАКИ СВИДЕТЕЛЬСТВУЮТ О НЕОБХОДИМОСТИ УПРЕЖДАЮЩЕЙ СТРАТЕГИИ ЗАЩИТЫ КИБЕРПРОСТРАНСТВА

Витаутас Бутримас, главный советник, Министерство национальной обороны Литвы

В 2010 году в г. Вильнюс (Литва) прошел Форум ООН по управлению Интернетом (IGF). Часть мандата IGF заключается в «обсуждении вопросов общественно-государственной политики, связанных с ключевыми элементами управления использованием Интернета с целью обеспечения устойчивости, защищенности, безопасности, стабильности и развития Интернета». Форум в Вильнюсе стал пятым ежегодным собранием с 2005 года. На нем в основном рассматривались вопросы защиты конфиденциальности передачи данных и свободы доступа к Интернету.

Однако очень мало внимания было уделено некоторым тревожным событиям в сфере кибербезопасности, произошедшим в период действия пятилетнего мандата IGF. Например, в 2007 году была совершена кибератака на интернет-инфраструктуру Эстонии, причем такого масштаба, что вся страна оказалась отключена от Интернета. В 2008 году Грузия пережила разрушительную кибератаку на информационно-коммуникационные системы, что привело к изоляции грузинского правительства и грузинского народа от остального мира. Эти атаки привели к значительным нарушениям конфиденциальности и свободы доступа к Интернету, являющихся объектом защиты со стороны IGF.

В киберпространстве происходило что-то серьезное. Неизвестные нарушители демонстрировали сложные и эффективные средства кибератак на критически важные системы связи и передачи информации. Еще больше настораживал тот факт, что никто так и не взял на себя ответственность за совершенные атаки. В данной статье будет проведена краткая оценка некоторых важных кибersобытий и тенденций для более полного понимания вопросов кибербезопасности, стоящих сегодня перед международным сообществом.

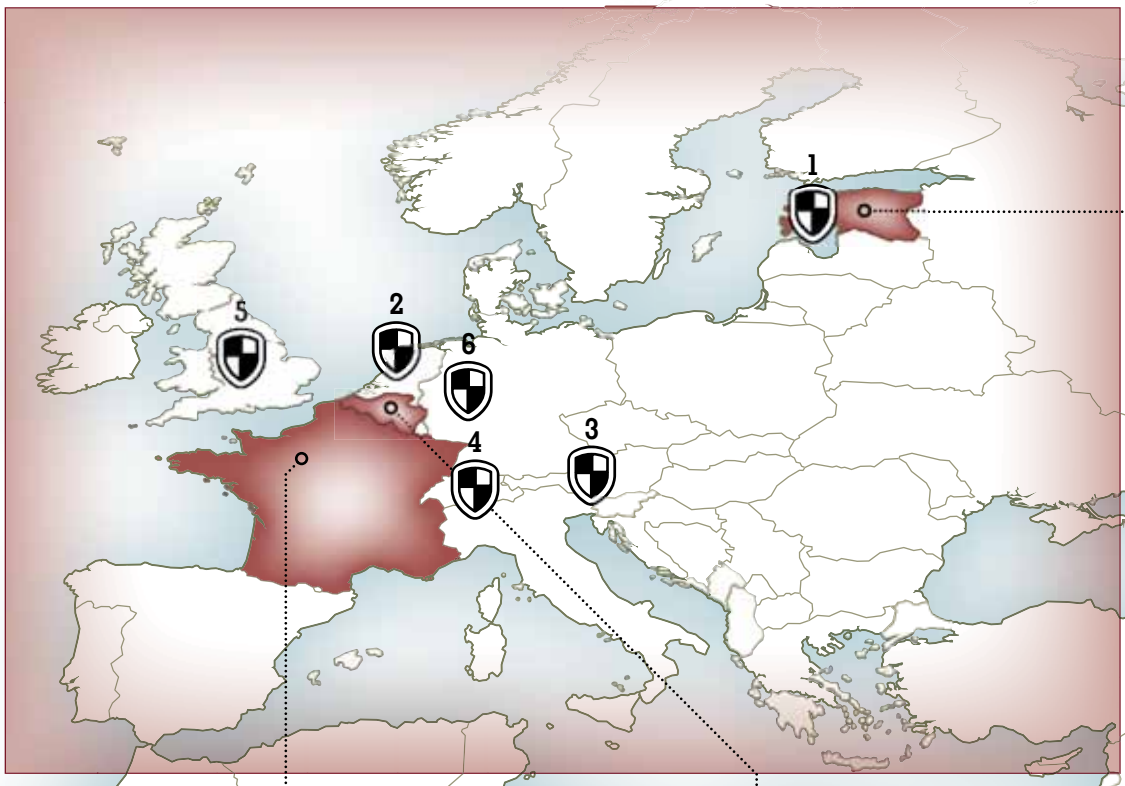
Вредоносные программы и киберпреступность

Написание вредоносных программ и взлом компьютерных систем более не являются занятием любителей или людей, делающих это в качестве хобби или в поисках признания. Причиняющие ущерб действия в киберпространстве стали достаточно безопасной и выгодной преступной деятельностью. Одним из факторов, позволяющих развиваться новой быстро растущей отрасли создания и распространения вредоносных программ и ботнетов (сетей из компьютеров-зомби), является то, что Интернет или киберпространство – это, по большей части, свободная и нерегулируемая среда.

Представьте себе, что киберпространство – это дорога или сеть магистралей. Однако в этой сети нет правил дорожного движения или полиции, штрафующей за превышение скорости или иным образом привлекающей нарушителей к ответственности. Даже если бы такая полиция и существовала в киберпространстве, то мы столкнулись бы с тем, что установить нарушителей практически невозможно. Злоумышленник уже давно покинул место преступления и не оставил никаких следов. В этом заключается проблема выявления источника. Очень сложно доказать, кто совершил то или иное преступление. Скорее всего, возможно выявить вредоносную программу или ботнет, однако, сам преступник и его компьютер остаются неизвестными.

Когда была проведена кибератака на Эстонию, местные специалисты догадывались, кто стоит за происходящим, но найти доказательства оказалось главной проблемой. Был составлен первый список компьютеров, с которых были совершены атаки, находившихся в таких неожиданных странах, как Египет, Вьетнам и Перу. Вероятнее всего, эти компьютеры были частью ботнета, контролируемого

НЕДАВНИЕ КИБЕРАТАКИ



Эстония
май 2007 г.

Грузия
август 2008 г.

Г. Париж (Франция)
Кибератака перед саммитом «Большой двадцатки».
Декабрь 2010 г.

Г. Брюссель (Бельгия)
крупная широкомасштабная кибератака перед саммитом Евросоюза, организованным для обсуждения вопросов экономики и ситуации на Ближнем Востоке.
Март 2011 г.

Иран
Стакснет
Лето 2010

ПРИМЕРЫ АГЕНТСТВ КИБЕРОБОРОНЫ

1 **НАТО**
Совместный центр обороны в сфере кибербезопасности
CCDCE

2 **Нидерланды**
Национальная инфраструктура по борьбе с киберпреступностью
NICC

3 **Австрия**
Австрийская программа обеспечения защиты объектов жизнеобеспечения
APCIP

4 **Швейцария**
Отчетно-аналитический центр обеспечения сохранности информации
MELANI

5 **Великобритания**
Центр защиты национальной инфраструктуры
CPNI

6 **Германия**
Национальный центр киберзащиты
NCAZ

«пастухом», ранее установившим свое ПО на слабозащищенные персональные компьютеры по всему миру.

Можно заработать деньги, используя вредоносные программы для совершения мошенничества, взлома банковских систем и получения контроля над кредитными картами и банковскими счетами людей. Киберпреступность продолжает набирать обороты. Согласно данным Национального центра США по борьбе с «беловоротничковой» преступностью, в 2009 году совершено более 330 тыс. киберпреступлений, что на 667 процентов превышает показатель за 2001 год.

Вредоносное ПО, способное совершать нападения и осуществлять взлом финансовых систем, имеет свою стоимость, как любой другой товар. «Пастух» (или управляющий ботнетом) использует вредоносные программы для заражения и получения контроля над другими компьютерами. Ботнеты продаются и сдаются в аренду, как любой другой товар, по ценам, регулируемым в зависимости от спроса и предложения. Таким образом, образовалась новая отрасль, ставшая одной из самых быстрорастущих в криминальном мире. Для взлома компьютеров и управления ботнетом требуются профессиональные навыки. Эти навыки пользуются спросом не только в мире киберпреступников, ищущих наживы, но также в государственном и частном секторах.

Угрозы социальных сетей

Социальные сети – это еще одно быстро развивающееся направление. Интернет предоставил человечеству новые возможности общения и обмена информацией. Можно свободно обмениваться фотографиями, видео и файлами в открытом доступе или с авторизацией для определенной группы. Социальные сети также становятся сценой для социального активизма. Например, в сети Facebook есть приложение под названием «Causes» (англ. «мотив, идея»), где могут собираться и вести деятельность заинтересованные стороны. Если вы не можете найти «cause» для обсуждения своей идеи, то можно осуществить поиск или создать новое приложение. Это приложение дает возможности для развития здорового демократического активизма, но что делать, если активизм носит разрушительный характер?

В одном из опубликованных примеров некий вебсайт призывал «добровольцев» бороться за свою идею. Желающие «подключиться к борьбе» должны были всего лишь загрузить предоставляемую на сайте программу, и программа сделает все остальное. На самом деле пользователь соглашался подключить свой компьютер к ботнету.

Социальные сети дают людям со сходными интересами возможность совместно действовать для развития демократии, однако при этом существует и темная сторона. Например, отдельные лица или группы могут использовать эту возможность для набора рекрутов в добровольческие «армии кибервоинов». Этот процесс крайне прост: для этого нужно всего лишь выполнить письменные инструкции или загрузить некое вредоносное ПО. Мы наблюдаем подобные процессы с 2007 года.

Кибератаки на Эстонию и Грузию

В 2007 году произошел раздел киберпространства. Пример с Эстонией показывает, что кибернападение на инфраструктуру государства, изначально подпитанное стихийно возникшими патриотическими чувствами, может позднее привлечь к себе и профессиональных киберпреступников. Это комбинация, обладающая большим потенциалом.

На первый взгляд кибератака казалась спонтанной патриотической реакцией россиян, вызванной перемещением памятника советскому воину-освободителю. Однако нападения продемонстрировали уровень

ОСНОВНЫЕ ВЕХИ

ПРОГРЕССА И РЕГРЕССА КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ И ИНТЕРНЕТА


APPLE

1976:
Основание компании «Apple Computer», ознаменовало начало эры персональных компьютеров.


WIKIPEDIA

1981:
«Microsoft Corp.» предлагает публике свою первую операционную систему.

1984:
Европейская организация ядерных исследований (ЦЕРН) начинает использовать Интернет-протокол для объединения своих внутренних компьютеров.

организации, способный временно парализовать внутренние сети и интернет-ссылки Эстонии. На вебсайтах были представлены объекты нападений и информация об атаке для тех, кто желал использовать свой компьютер в общей «борьбе». Управляющие ботнетами использовали вредоносные программы для заражения компьютеров ничего не подозревающих жертв, и армии «зомби» «открыли огонь» по сайтам эстонских банков, правительства и прессы.

В августе 2008 года использование сети компьютеров для временного подрыва информационно-коммуникационной инфраструктуры государства приняло новую и потенциально более опасную форму – речь идет о совершении кибератаки во время проведения традиционной военной операции. В нем были использованы некоторые элементы кибератаки, проведенной в Эстонии годом ранее: патриотизм простого народа, разожженный с помощью социальных сетей; использование профессиональных «пастухов» ботнетов и элементов организованной преступности. В результате был нанесен хорошо спланированный, точно рассчитанный по времени разрушительный кибердар по системам связи и передачи информации грузинского правительства и частного сектора. Этой атакой удалось отрезать доступ к информации о том, что происходило в стране. Была нарушена ежедневная деловая активность; люди испытывали страх и неуверенность в будущем. Короче говоря, возможность Грузии организовывать и координировать свою национальную оборону была поставлена под угрозу.

Анализ кибератаки на Грузию показывает, что данное событие также положило начало более страшной тенденции – возможности физического уничтожения жизненно важных компонентов командно-информационных систем. Согласно результатам исследования, атака могла иметь значительно более вредоносный характер, однако нарушители предпочли оставаться в выбранных рамках. К сожалению, организаторы кибератаки извлекли для себя важный урок: кибердар – по-прежнему, привлекательное оружие, и никто не знает, что делать в таких случаях.

«Стакснет»: первая межконтинентальная кибератака?

Появившийся в 2009 году вирус «Стакснет», о котором средства массовой информации рассказали летом 2010 года, стал новым «рецептом киберрагу», в состав которого вошли все ранее известные ингредиенты профессиональных кибернавыков. В опубликованном анализе «Стакснета» говорится, что данный червь создан на основе серьезных исследований и отличается своей сложностью. Червь продемонстрировал на практике, что он способен не только временно нейтрализовать объект нападения, но и уничтожить его физически.

В одном из исследований говорится, что для создания такого червя требуются значительные ресурсы (профессионалы киберсферы и средства разведки), предоставить которые под силу только правительству. Одной из целей нападения «Стакснета» могли стать иранские ядерные объекты, системы контроля и сбора данных (SCADA) которых, используемые для управления важнейшими операциями, были изготовлены компанией «Siemens».

Сложно сказать, справился ли «Стакснет» с той деструктивной задачей, для которой был создан. Вирус появился в других странах, при этом заявлений о нанесении ущерба ядерным объектам не последовало.

Результаты другого исследования говорят о том, что «Стакснет» был разработан как психологическое оружие и в этом качестве, вероятно, соответствовал своему назначению. Представьте себе, что есть возможность донести до своего противника следующее сообщение: «Нам не нравится то, чем вы занимаетесь на этом объекте; мы можем управлять им без вашего ведо-


THINKSTOCK

1986:

Первым успешным случаем «установления авторства» кибератаки считается раскрытие астрономом Клиффордом Столлом хакерских нападений КГБ на данные Стратегической оборонной инициативы США.


ROANOKE COLLEGE

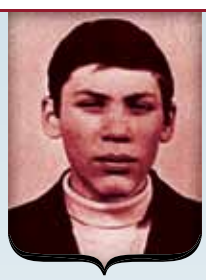
1989:

Компания «McAfee Associates» выводит на рынок свое первое антивирусное программное обеспечение. Первые 100 тыс. пользователей начинают использовать Интернет.

THINKSTOCK

1991:

Официальное появление «всемирной паутины» World Wide Web (WWW).



1994:

Российский хакер Владимир Левин совершает ограбление крупных корпораций, взломав электронные счета «Ситибанка».

ма, и, кстати, рекомендуем поосторожнее обращаться с кнопками». Как и в предыдущих кибersобытиях, создатели «Стакснета» остались неизвестны. Может быть, на месте преступления и не осталось улик, но преступники почувствовали слабость противника. Если «Стакснет» и его варианты являются новой формой кибератак, то перед нами – новая и более опасная проблема.

Кибератака в Мьянме накануне выборов

В первую неделю ноября 2010 года Мьянма готовилась к выборам, проводившимся впервые за последнее двадцатилетие. Выборы получили широкое освещение в прессе, однако одно событие осталось практически без внимания. За неделю до выборов информационная инфраструктура Мьянмы пережила массивную распределенную атаку типа «отказ в обслуживании», которая привела к отключению Мьянмы от Интернета. Можно только предположить, как это сказалось на выборах в стране. Однако в том, что касается кибернетической части, данная атака вызвала беспокойство в отношении внезапно возросших кибервозможностей. Нападение на Мьянму было в несколько раз более мощным по сравнению с атаками на Эстонию и Грузию. Данное укрепление «киберсилы» представляет собой тревожную тенденцию.

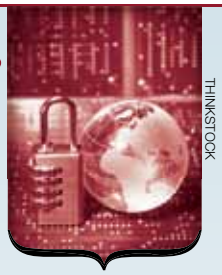
Выводы

Зависимость государства от систем связи и передачи информации и его уязвимость перед угрозой подрыва или уничтожения информационной инфраструктуры посредством вредоносных программ, направленных из неизвестного источника неизвестным злоумышленником, привели к новой и привлекательной форме нападения на государство. Такого рода атаки особенно привлекательны для правительств, не способных добиться своих внешнеполитических целей приемлемыми с точки зрения международного сообщества способами.

Данная возможность злоупотребления Интернетом может иметь настолько широкое применение, что государству сложно удержаться от соблазна воспользоваться ей. Можно секретно запустить атаку через третьих лиц, практически на 100 процентов опровергнув свое участие независимо от того, станет ли данная атака известна общественности. Ущерб от нападения может заключаться как в кратковременном подрыве систем, так и в физическом разрушении интернет-инфраструктуры. «Командующие» этими арсеналами себя не афишируют, но они доступны для тех, кто заинтересован в их услугах. Можно сколько угодно говорить об отсутствии прямых доказательств участия правительств, однако и косвенных улик достаточно, чтобы сделать вывод о том, что в некоторой степени они в этом замешаны.

Поскольку ботнеты и вредоносные программы в состоянии подорвать важнейшие объекты информационной инфраструктуры государства, киберугроза является проблемой национальной безопасности. Это признается и государствами, находящимися в зависимости от Интернета, и теми, кто пытается воспользоваться этой уязвимостью. Признав данную угрозу, правительства начинают сотрудничать в борьбе с киберпреступностью. Многие, однако, также соперничают в «гонке кибервооружений».

Сама интернет-отрасль может непроизвольно облегчить организацию и проведение кибератак. Например, компания «Microsoft» объявила о подписании Соглашения о сотрудничестве в области безопасности компьютерных технологий с Россией, что, помимо прочего, обеспечило доступ к исходному коду операционной системы «Windows». Такое же соглашение было подписано с Китаем в 2007 году, и прошлым летом российское правительство получило доступ к коду последней операционной системы «Windows». Конечно, можно понять рыночные мотивы действий «Microsoft», однако также совсем не сложно понять, что если код



1995:
«Strano Network» совершает кибератаку на компьютеры правительства Франции и становится одной из первых хакерских групп.

1996:
Финская компания «Nokia» выпускает первый сотовый телефон с возможностью подключения к Интернету.

1998:
«Google» создает свою первую поисковую систему.

2000:
К этому времени в Интернете зарегистрировано 10 миллионов доменных имен. Разработанный на Филиппинах компьютерный червь «Love Bug» поражает компьютеры по всему миру.

попадет не в те руки, он может быть использован для нахождения слабых мест в программе и новых направлений и возможностей кибернападений.

Как устранить эту новую угрозу национальной безопасности и избежать возможной гонки кибервооружений? Для начала правительство и отрасль должны осознать свою двойную роль – как части решения и как части проблемы. Можно предусмотреть ограничения в рамках «договора о контроле над кибервооружениями». Однако чтобы быть эффективными, договоры должны поддаваться проверке и иметь юридическую силу. Необходимо обозначить главные заинтересованные стороны, представляющие государственный и частный сектор, а также международное сообщество, и применить соответствующие инструменты для согласования их действий. Целью может стать создание сети для сбора разведданных и сети сообщений для обмена информацией, что привело бы к выявлению киберпреступников и организаторов нападений. Это могло бы стать надежным решением проблемы обнаружения источника. Если станет возможно найти исполнителя атаки, то тогда, скорее всего, и «серые кардиналы» будут вынуждены взвешивать выгоды и цену нападения. После обнаружения организаторов атак необходимо использовать международный инструмент для оказания давления и, при необходимости, применения наказания.

Можно назвать это «интернет-полицией», если хотите. Государства должны заставлять провайдеров услуг и отдельных лиц отвечать за свои поступки. Если они не согласны действовать в соответствии с правилами, должны применяться санкции. Мы должны заставить организаторов кибератак задуматься.

Международные действия требуют времени, однако первые шаги можно предпринять уже сейчас на местном уровне: создать сеть взаимодействия сетевых специалистов, представляющих все заинтересованные сектора, включая правительство, банки, энергетическую и транспортную промышленность, коммерческие объекты и телекоммуникации. Правительство должно быть во главе, поскольку оно, естественно, более всех заинтересовано в развитии национальной стратегии кибербезопасности.

Эта лига экспертов, представляющая все заинтересованные в кибербезопасности стороны, должна стать первым фронтом национальной кибероборонны. Общение во время встреч и консультации повысят доверие между указанными сторонами, что улучшит обмен информацией и уровень знаний, которые можно использовать в случае чрезвычайной ситуации в киберпространстве. Меморандум о взаимопонимании в вопросах сотрудничества между заинтересованными сторонами мог бы обеспечить более слаженную и скоординированную реакцию на киберпроисшествия.

Не нужно ждать кризиса, чтобы устранять его последствия с помощью специально созданной антикризисной группы. В мае 2007 года на совместной рабочей встрече между НАТО и «Microsoft», проведенной в Редмонде (штат Вашингтон, США), представитель Эстонии поднялся на подиум и заявил, что его «страна переживает кибератаку». После целой ночи звонков в столицы постепенно поступили предложения о помощи, но все было сделано спонтанно. С тех пор в управлении киберкризисами был достигнут некоторый прогресс помимо использования подхода, заключающегося в создании специальных антикризисных групп.

Кибербезопасность и Интернет находятся на перепутье. То, как мы сегодня решаем вопросы кибербезопасности, определит не только степень сохранения свободы доступа и конфиденциальности данных в киберпространстве, но также и степень защищенности наших объектов киберинфраструктуры. Однако было бы недостаточно решить только проблемы киберпреступности или ограничить использование Интернета террористами в целях получения информации и набора рекрутов. Перефразируя Сунь-Цзы, чтобы победить, мы должны понимать своего врага (и самих себя). □


AGENCE FRANCE-PRESSE

2001:
Шотландский хакер Гари Маккиннон взламывает десятки компьютеров, принадлежащих оборонным ведомствам, что стало «крупнейшим взломом военных компьютеров в истории».


THINKSTOCK

2007:
Количество веб-пользователей в мире превысило 1 миллиард.

2009:
Проведена китайская шпионская компьютерная операция под названием «Ghostnet» с целью проникновения в компьютерные сети, расположенные более чем в 100 странах.

2011:
Группа «анонимных» хакеров взламывает серверы «Sony» и «Банка Америки» и опубликовывает полученную конфиденциальную информацию.

Остановить кибертерроризм

ГОСУДАРСТВА ДОЛЖНЫ ОБЪЕДИНИТЬ УСИЛИЯ ДЛЯ УСПЕШНОЙ БОРЬБЫ С ИНТЕРНЕТ-ПРЕСТУПНИКАМИ

Д-р Вячеслав Дзюндзюк, профессор Харьковский региональный институт Национальной академии государственного управления (Украина)

ИЛЛЮСТРАЦИЯ PER CONCORDIAM

Кибернетической преступностью называются преступления, совершаемые в так называемом «виртуальном пространстве». Виртуальное пространство (или кибернетическое пространство) можно определить как моделируемое компьютером информационное пространство, в котором содержатся сведения о лицах, предметах, фактах, событиях, явлениях и процессах, представленные в математическом, символьном или любом другом виде и находящиеся в процессе движения по локальным и глобальным компьютерным сетям, либо сведения, хранящиеся в памяти любого физического или виртуального устройства, а также другого носителя, специально предназначенного для их хранения, обработки и передачи.[1]

В отличие от традиционных видов преступлений, таких как убийство или кража, история которых насчитывает многие столетия, кибернетическое преступление представляет собой относительно недавнее явление, появившееся после создания интернета. Стоит отметить, что сама природа интернета способствует совершению преступлений. Его глобальный охват, способность преодолевать границы и достигать широкой аудитории, анонимность его пользователей, а также распределение и взаимозаменяемость основных сетевых узлов дают преступникам преимущество и позволяют им эффективно скрываться от правоохранительных органов.

Первые компьютерные преступники, позднее названные «хакерами», появились в 1970-х годах. Трудно с полной уверенностью сказать, кто был самым первым хакером, но в большинстве источников первым профессиональным хакером называется Джон Дрейпер. Он также создал первую хакерскую «специализацию» – так называемое «фрикерство», сокращение от английских слов «phone hacking» («телефонный хакинг»). Среди хакеров тех времен были и такие известные сейчас люди как Стив Возняк и Стив Джобс, которые впоследствии основали корпорацию Apple. *Они наладили производство устройств, позволявших взламывать телефонные сети. Можно считать, что именно в этот период началось развитие компьютерной преступности.*

Первый широко освещенный арест виртуального преступника был произведен в 1983 году в городе Милуоки в США. Это был первый зафиксированный случай взлома в интернете, совершенного шестью подростками, называвшими себя «Группа 414» (414 – это телефонный код города Милуоки). В течение девяти дней они взломали 60 компьютеров, некоторые из которых принадлежали Лос-Аламосской национальной лаборатории. После ареста группы один из ее членов дал показания против остальных, которые впоследствии получили условные сроки.[2]

В 1980-е годы наблюдается значительный рост числа компьютерных атак. Так, например, пользователями интернета в CERT (Computer Emergency Response Team – организацию, следящую за угрозами сетевой безопасности) было направлено всего шесть жалоб на компьютерные атаки в 1988 году (год основания организации), 132 жалобы – в 1989 году и 252 жалобы – в 1990 году. Кибернетические преступления перестали быть редкостью, на сцену вышли крупные группы хакеров, а интернет стал использоваться для совершения более широкого спектра преступлений. *Это стало началом второй фазы развития кибернетической преступности, для которой характерно расширение специализации интернет-преступников.*

В 1984 году Фред Коэн опубликовал статью о создании первых вредоносных самовоспроизводящихся компьютерных программ, в которой для их описания был предложен термин «компьютерный

вирус». Он также написал программу, демонстрировавшую возможность заражения одного компьютера другим.

В 1986 году был арестован член группы «Легион смерти» («Legion of Doom») Ллойд Блэнкеншип, известный как «Ментор». Находясь в заключении, он написал широко известный «Манифест хакера».[3] Выраженные в этом манифесте идеи и ценности до сих пор считаются основой идеологии и культуры хакеров и широко распространены по всему интернету. Очевидно, количественный рост кибернетической преступности совпал с увеличением популярности хакерской идеологии в компьютерном мире, что свидетельствует о наличии связи между этими явлениями.

В 1994 году мир узнал о деле Владимира Левина, которое следователи охарактеризовали как «транснациональное сетевое преступление». Международная преступная группа в составе 12 человек использовала интернет и сеть передачи данных Sprint/Telenet для взлома систем защиты и совершения более 40 переводов на общую сумму 10,7 миллионов долларов со счетов клиентов различных банков в девяти странах мира на свои счета в банках США, Финляндии, Израиля, Швейцарии, Германии, России и Нидерландов.[4] Это было первым крупным международным финансовым преступлением, совершенным при помощи интернета, ставшим известным широкой публике. Данный случай продемонстрировал, что кибернетические преступления могут причинить серьезный финансовый урон.

В 1998 году 12-летний хакер проник в компьютерную систему, контролирующую паводковые шлюзы плотины Теодора Рузвельта в Аризоне. Открытие шлюзов на плотине могло привести к затоплению городов Темпе и Меса в штате Аризона, с общим населением в миллион человек.[5] Этот случай породил такие термины, как «интернет-терроризм», «компьютерный терроризм» и «кибертерроризм». Он также продемонстрировал, что сам интернет крайне уязвим для кибернетических атак, так как его ключевая инфраструктура доступна из любой точки мира, – факт, о котором хакеры прекрасно осведомлены.

Международная угроза

Возникновение кибертерроризма и широко освещаемых преступлений, совершаемых международными преступными группами, свидетельствует о том, что кибернетическая преступность стала транснациональной. Это является началом третьей фазы развития кибернетической преступности.

Тревожным фактом является то, что с развитием интернета не только международные кибернетические атаки, но и беспечность профессионалов может иметь серьезные последствия. Например, в 1997 году ошибка сотрудника компании Network Solutions привела к тому, что все сайты с адресами, заканчивающимися на «.net» или «.com», стали недоступны. То есть небрежность со стороны одного лишь человека нарушила работу всей Всемирной сети.

В то же время кибернетические атаки становятся средством достижения политических целей. Типичным примером служит атака типа «отказ в обслуживании» при помощи интернета: злоумышленники одновременно заходят на сайт, подключаются к серверу, посылают электронные сообщения или пишут сообщения на форумах с целью затруднить или даже сделать невозможным доступ к сайту со стороны других пользователей. Такой веб-сайт или сервер оказывается перегруженным запросами, что приводит к перебоям в его работе или к полному ее прекращению.

Первая атака такого рода была осуществлена группой, называющей себя «Strano Network», протестовавшей против политики французского правительства в ядерной и социальной сферах. 21 декабря 1995 года эта группа в течение часа атаковала сайты различных правительственных агентств. Участники группы с разных континентов были проинструктированы следующим образом: им полагалось, всем одновременно, с помощью браузеров заходить на правительственные сайты. В результате некоторые сайты действительно были недоступны некоторое время.[6]

Все шире проявляются транснациональные аспекты киберпреступности. Конфликт в Косово считается первой интернет-войной, в ходе которой различные группы компьютерных активистов использовали интернет для того, чтобы выразить свое осуждение действий как Югославии, так и НАТО, путем нарушения работы правительственных компьютерных систем и получения контроля над веб-сайтами с последующим искажением их внешнего вида (т.н. «deface сайта»). Параллельно в интернете циркулировали рассказы об опасностях и ужасах войны, а политики и общественные деятели использовали интернет для того, чтобы их призывы достигли как можно более широкой аудитории по всему миру.[7] Все эти черты характерны для третьей фазы развития кибернетической преступности.

Следует отметить, что сегодня практически любой военный или политический конфликт сопровождается организованным противостоянием в интернете. Так, например, в 2005 году в Японии был опубликован новый школьный учебник истории, содержащий искаженное изложение событий в Китае в 1930-1940-х годах, не затрагивающее военные преступления, совершенные японскими силами в ходе этой интервенции, что вызвало целую волну кибернетических атак. Среди целей этих атак были японские министерства и правительственные агентства, сайты крупных японских корпораций и сайты, посвященные Второй мировой войне. В данном случае китайские хакеры продемонстрировали высокую степень организованности, проявившуюся в синхронности и массовом характере их атак. С учетом того, что в Китае интернет контролируется государством, предполагается, что данная атака была санкционирована правительством Китая. *Использование кибернетических атак в политических целях может считаться началом четвертой фазы развития кибернетической преступности.*

Пример Китая был скопирован российскими хаке-

рами, осуществившими несколько DDoS-атак (распределенных атак типа «отказ в обслуживании»). В течение нескольких дней в конце апреля – начале мая 2007 года атакам подверглись эстонские правительственные сайты. Ответственность за эти атаки взяло на себя молодежное движение «Наши».[8] А в августе 2009 года американское издание Aviation Week обвинило российских хакеров в нападении на сервер трубопровода «Баку — Тбилиси — Джейхан». В статье говорилось, что эти атаки проводились с тех же адресов, что и атаки на эстонские сайты.[9]

Характеристики кибертерроризма

В наши дни терроризм носит международный характер и, в соответствии с рядом международных правовых норм, считается международным преступлением. Это тем более верно в отношении новой разновидности терроризма – кибертерроризма.

Следует отметить, что средства массовой информации зачастую используют термин «кибертерроризм» некорректно, создавая путаницу в понятиях, смешивая термины «хакер» и «кибертеррорист». Однако это является ошибкой. Терроризм является преступлением, но не любое преступление является терроризмом, так же как кибертеррорист может быть хакером, но не каждый хакер осуществляет террористические акты в киберпространстве.

Считается, что термин «кибертерроризм» появился в 1997 году. В этом году специальный агент ФБР Марк Поллитт определил кибертерроризм как “преднамеренную политически мотивированную атаку на информационные, компьютерные системы, компьютерные программы и данные, результатом которой является насилие по отношению к гражданским целям со стороны субнациональных групп или тайных агентов”.[10]

Известный эксперт Дороти Деннинг говорит о кибертерроризме как о «противоправной атаке или угрозе атаки на компьютеры, сети или хранящуюся в них информацию.., совершенной с целью принудить правительство или население к содействию в достижении политических или социальных целей».[11]

Исследователи Мэтью Девост, Брайан Хьютон и Нил Поллард определяют информационный терроризм (разновидностью которого является кибертерроризм) как:

1. Соединение преступного использования информационных систем при помощи мошенничества или злоупотреблений и физического насилия, свойственным терроризму;
2. Сознательное злоупотребление цифровыми информационными системами, сетями или компонентами этих систем или сетей в целях, которые способствуют осуществлению террористических операций или актов.[12]

Можно выделить три вида кибертерроризма:

1. Совершение террористических действий с помощью компьютеров и компьютерных сетей (терроризм в «чистом виде»);
2. Использование кибернетического пространства в целях террористических групп, но не для непосредственного совершения терактов. (По этому поводу директор ЦРУ Джордж Тенет сказал, что такие террористические группы как Хезболла, Хамас, Абу-Нидаль и Аль-Каида активнейшим образом используют возможности компьютеров для организации своей деятельности.)[13]
3. Совершение в киберпространстве действий, не преследующих политические цели, но представляющих угрозу национальной или общественной безопасности.

Первому виду кибертерроризма можно дать определение с помощью соединения понятий «кибернетическое пространство» и «кибернетический терроризм».

Таким образом, кибертерроризм в этом значении есть умышленная, политически мотивированная атака на обработанную компьютером информацию, компьютерную систему или сеть, являющаяся угрозой для жизни и здоровья людей или приводит к другим общественно опасным последствиям, в случае если она была совершена в целях нарушения общественной безопасности, устрашения населения, провоцирования военного конфликта или оказания воздействия на принятие решений органами власти в преступных целях. В последнем случае кибертерроризм может выражаться в угрозе применения насилия для поддержания состояния постоянного страха с целью достижения политических или иных целей, принуждения к определенным действиям или привлечения внимания к отдельному кибертеррористу или к террористической организации, к которой он принадлежит. В этом случае причинение вреда или угроза причинения вреда служит своего рода предупреждением о возможности еще более серьезных последствий в случае невыполнения требований террориста.

Что же касается второго вида кибертерроризма, то вопрос отнесения к кибертерроризму использования кибернетического пространства террористическими группами для осуществления и популяризации своей деятельности, но не для непосредственного совершения терактов, является спорным. Конечно, в соответствии с уголовным кодексом, данные действия вряд ли можно квалифицировать как терроризм, но если руководствоваться здравым смыслом, то причисление данных действий к кибертерроризму кажется логичным и, по-видимому, будет осуществлено в недалеком будущем. Данный вид кибертерроризма может включать такие вещи, как:

- Сбор с помощью Интернета подробной информации о предполагаемых целях, их местонахождении и характеристиках.
- Создание сайтов с подробной информацией о террористических движениях, их целях и задачах, публикация на этих сайтах данных о времени встречи людей, заинтересованных в поддержке террористов, указаний о формах протеста и т.п., т.е. синергетическое воздействие на деятельность групп, поддерживающих террористов.
- Использование Интернета для обращения к массовой

аудитории для сообщения о будущих и уже спланированных действиях на страницах сайтов или рассылка подобных сообщений по электронной почте, а также предание террористами с помощью Интернета широкой гласности своей ответственности за совершение террористических актов.

- Использование Интернета для информационно-психологического воздействия, в том числе инициация «психологического терроризма». С помощью Интернета можно посеять панику, ввести в заблуждение, привести к разрушению чего-либо. Всемирная сеть — благодатная почва для распространения различных слухов, в том числе и тревожных, и эти возможности сети также используются террористическими организациями.
- Сбор денег для поддержки террористических движений.
- Вымогательство денег у финансовых институтов, чтобы те могли избежать актов кибертерроризма и не потерять свою репутацию.
- Вовлечение в террористическую деятельность ничего не подозревающих соучастников – например, хакеров, которым не известно, к какой конечной цели приведут их действия. Кроме того, если раньше сеть террористов обычно представляла собой разветвленную структуру с сильным центром, то теперь это сети, где не просматривается четкая иерархия – такую возможность предоставляет Интернет.
- Размещение в Интернете сайтов террористической направленности, содержащих информацию о взрывчатых веществах и взрывных устройствах, ядах, отравляющих газах, а также инструкции по их самостоятельному изготовлению. Лишь в одном русскоязычном сегменте интернета существуют десятки сайтов, на который можно найти информацию подобного рода.
- Использование интернета в качестве средства связи, а именно, использование услуг электронной почты или электронных досок объявлений для отправки зашифрованных сообщений. В частности, Рамзи Юсеф, организовавший взрыв Всемирного торгового центра, получал инструкции по организации террористических актов зашифрованными посланиями прямо на свой лэптоп. Другие террористические группы, такие как «Черные тигры» (их обычно связывают со шриланкийской группировкой «Тигры Освобождения Тамил Илама») атакуют правительственные вебсайты и адреса электронной почты.
- Перенесение баз подготовки террористических операций. Терроризм больше не ограничен территорией того государства, где скрываются террористы. Более того, базы подготовки террористических операций уже, как правило, не располагаются в тех странах, где находятся цели террористов.[14]

Что касается третьего вида кибертерроризма, то действия, которые могут быть совершены хулиганами, не преследующими политических целей, но которые, тем не менее, могут представлять угрозу для общественной и/или национальной безопасности, также можно рассматривать как терроризм. К этой категории кибертерроризма можно отнести намеренное распространение вирусов, троянских программ, сетевых червей и так далее, либо вторжение с целью нарушения работы правительственных или общественных институтов. Вот два примера.

Вирус «I Love You»

Компьютерный вирус, известный под названием «I Love You» (или «Love Bug»), был запущен в интернет 1 мая 2000 года в Азии и с удивительной скоростью распространился по всей планете. Он нарушил работу правительственных учреждений, парламентов и корпораций во многих странах мира, заразив около 45 миллионов компьютерных сетей. Так, например, в США этот вирус поразил компьютерные сети четырнадцати федеральных агентств, включая ЦРУ, Министерство обороны, Белый дом и Конгресс.[15] Он также нарушил компьютерную сеть Британского парламента. За пять дней, последовавшие за его появлением, вирус причинил материальный ущерб на общую сумму 6,7 миллиардов долларов. Поэтому неудивительно, что организация Computer Economics классифицировала вирус «I Love You» как акт кибертерроризма.

В том же мае 2000 года был вынесен приговор Франклину Адамсу из Хьюстона, распространившему «сетевого червя», который перепрограммировал модемы зараженных компьютеров на автодозвон до службы спасения 911. В результате несколько тысяч компьютеров в больницах, полицейских и пожарных участках были выведены из строя, что, очевидно, представляло угрозу общественной безопасности.

К сожалению, в результате анализа мировых тенденций развития кибертерроризма можно с большой долей вероятности предположить, что эта угроза будет расти с каждым годом. Технический прогресс происходит столь стремительно, что общество не успевает осознавать некоторые из его последствий; исправление ситуации требует значительных усилий. К тому же постоянно возрастает зависимость от компьютерных систем и информационных технологий.

Таким образом, можно утверждать, что кибертерроризм представляет собой серьезную угрозу для человечества, сравнимую с угрозой ядерного, биологического и химического оружия, однако по причине своего недавнего возникновения размер этой угрозы еще не до конца признан и изучен. Мировой опыт в данном вопросе очевидным образом свидетельствует о неоспоримой уязвимости всех без исключения стран, особенно учитывая, что для кибертерроризма не существует государственных границ и что кибертеррорист может угрожать информационным системам, расположенным практически в любой точке мира. А найти и нейтрализовать кибертеррориста крайне трудно по причине скудости оставляемых им улик, в отличие от реального мира, в котором собрать оставшиеся после преступления улики зачастую намного легче.

Меры борьбы с кибернетическими угрозами

Все это приводит к тому, что для борьбы с кибертерроризмом и вообще с кибернетической преступностью требуется широкий спектр мер. В зависимости от области их приложения эти меры можно разделить на несколько категорий:

- Законодательные – В этой области кое-что уже сделано и делается в настоящее время. Так, например, законодательные органы многих стран приняли специальные законы о компьютерных и интернет-преступлениях; более того, законодательство в области компьютерных преступлений становится отдельной областью законодательства, отличающейся суровостью наказаний. Постепенно принимаются международные законодательные акты, регулирующие отношения в интернете и направленные на борьбу с кибернетической преступностью, – например, Европейская конвенция о компьютерных преступлениях. Дальнейшее усовершенствование законодательства, особенно международного, в сфере борьбы с кибернетической преступностью, несомненно, поможет бороться с этим явлением.
- Организационные – То есть эффективное сотрудничество государств с другими государствами, их правоохранительными органами и спецслужбами, а также с международными организациями, задачей которых является борьба с кибертерроризмом и транснациональной компьютерной преступностью. Также существует необходимость в создании единой международной организации, такой, каким является Интерпол, в руках которой была бы сконцентрирована борьба с кибернетической преступностью. Некоторые страны уже объединили свои усилия в этом направлении, но это сотрудничество нуждается в расширении и углублении.
- Технологические – Без сомнения, нужно двигаться в направлении совершенствования технологий защиты общества от кибернетических преступлений и реагирования на них, так как это позволит помешать преступникам в достижении их целей или даже собственно совершению преступлений. Развитию таких технологий может содействовать эффективное сотрудничество между государственными институтами и частными компаниями, работающими в области высоких технологий и разработки программного обеспечения, а также с экспертами в области компьютерных технологий. Такого рода совместные усилия позволят нам оставаться на шаг впереди противника вместо того, чтобы просто реагировать на его действия.

Все три перечисленных выше направления деятельности важны и могут привести к значительным успехам в борьбе с киберпреступностью. В принципе определенная работа продолжается во всех этих направлениях. Однако парадокс заключается в том, что реализация этих мер приводит к усилению именно тех характеристик кибернетического пространства, которые как раз и делают возможным совершение кибернетических преступлений: глобальный охват, доступность и постоянное развитие технологий. Тем не менее, существует еще один путь, которому, на мой взгляд, уделяется недостаточно внимания со стороны правительственных организаций: а именно, уменьшение базы кибернетической преступности, то есть количества лиц, совершающих кибернетические преступления. Этого можно было бы добиться с помощью целевой переориентации их ценностей. Но эта область деятельности требует отдельного рассмотрения, выходящего за пределы настоящей статьи.

Таким образом, можно констатировать, что, к сожалению, развитие компьютерных и телекоммуникационных сетей (в особенности интернета и порожденных на его основе социальных взаимоотношений) характеризуется постоянным ростом числа преступных и социально опасных действий в кибернетическом пространстве. Высокие социальные издержки таких деяний вызваны, в первую очередь, их транснациональной природой, благодаря которой последствия этих деяний могут затронуть неограниченное число людей в самых разных странах.

Принимая во внимание данную глобальную негативную тенденцию, для борьбы с кибернетическими угрозами и их предотвращения требуется широкий спектр решительных действий, учитывающих проникновение интернета и «виртуального мира» во все сферы жизни. Это должно стать основным направлением усилий по обеспечению информационной безопасности и национальной безопасности в целом. □

1. Голубев В.А. «"Кибертерроризм" – миф или реальность?» http://www.crime-research.org
2. Лукацкий А. «Хакеры управляют реактором», Computer Crime Research Center, http://www.crime-research.org/library/Lukac0103.html
3. Ментор. «Манифест хакера», 8 января 1986 http://project.cyberpunk.ru/idb/hacker_manifesto.html
4. Кураков Л.П., Смирнов С.Н. «Информация как объект правовой защиты», М., Гелиос, 1998, стр. 220-221.
5. Роберт Лемос. «Кибертерроризм: реальный риск» («Cyberterrorism: The real risk»), Computer Crime Research Center http://www.crime-research.org/library/Robert1.htm
6. Деннинг Д. «Активность, хактивизм и кибертерроризм: Интернет как средство воздействия на внешнюю политику» («Activity, Hactivity and Cyberterrorism: The Internet as a Means of Influence on Foreign Policy»). Владивостокский центр исследования организованной преступности, перевод Т.Л. Тропиной http://www.crime.vl.ru/index.php?p=1114&more=1&c=1&tb=1&pb=1
7. Андреев А., Давыдович С. «Об информационном противоборстве в ходе вооруженного конфликта в Косово», Центр практической психологии «ПСИ-ФАКТОР» http://www.psyfactor.org/warkosovo.htm
8. См. http://www.lenta.ru/news/2009/03/12/confess
9. См. http://www.securitylab.ru/news/384118.php
10. Красавин С. «Что такое кибертерроризм?» («What is Cyber-terrorism?») http://rr.sans.org/infowar
11. Деннинг Д. «Активизм, хактивизм и кибертерроризм: Интернет как инструмент воздействия на внешнюю политику» («Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy») http://www.nautilus.org/info-policy/workshop/papers/denning.html
12. Томас Т.Л. «Сдерживание асимметричных террористических угроз, стоящих перед обществом в информационную эпоху» // «Мировое сообщество против глобализации преступности и терроризма. Материалы международной конференции», М., 2002, стр. 165.
13. Рональд Л. Дик. «О проникновении в правительственные компьютерные сети» («Issue of Intrusions into Government Computer Networks») http://www.fbi.gov/congress/congress01/rondick.htm
14. Томас Т.Л. «Сдерживание асимметричных террористических угроз, стоящих перед обществом в информационную эпоху» // «Мировое сообщество против глобализации преступности и терроризма. Материалы международной конференции», М., 2002
15. Рональд Л. Дик «О проникновении в правительственные компьютерные сети» («Issue of Intrusions into Government Computer Networks») http://www.fbi.gov/congress/congress01/rondick.htm

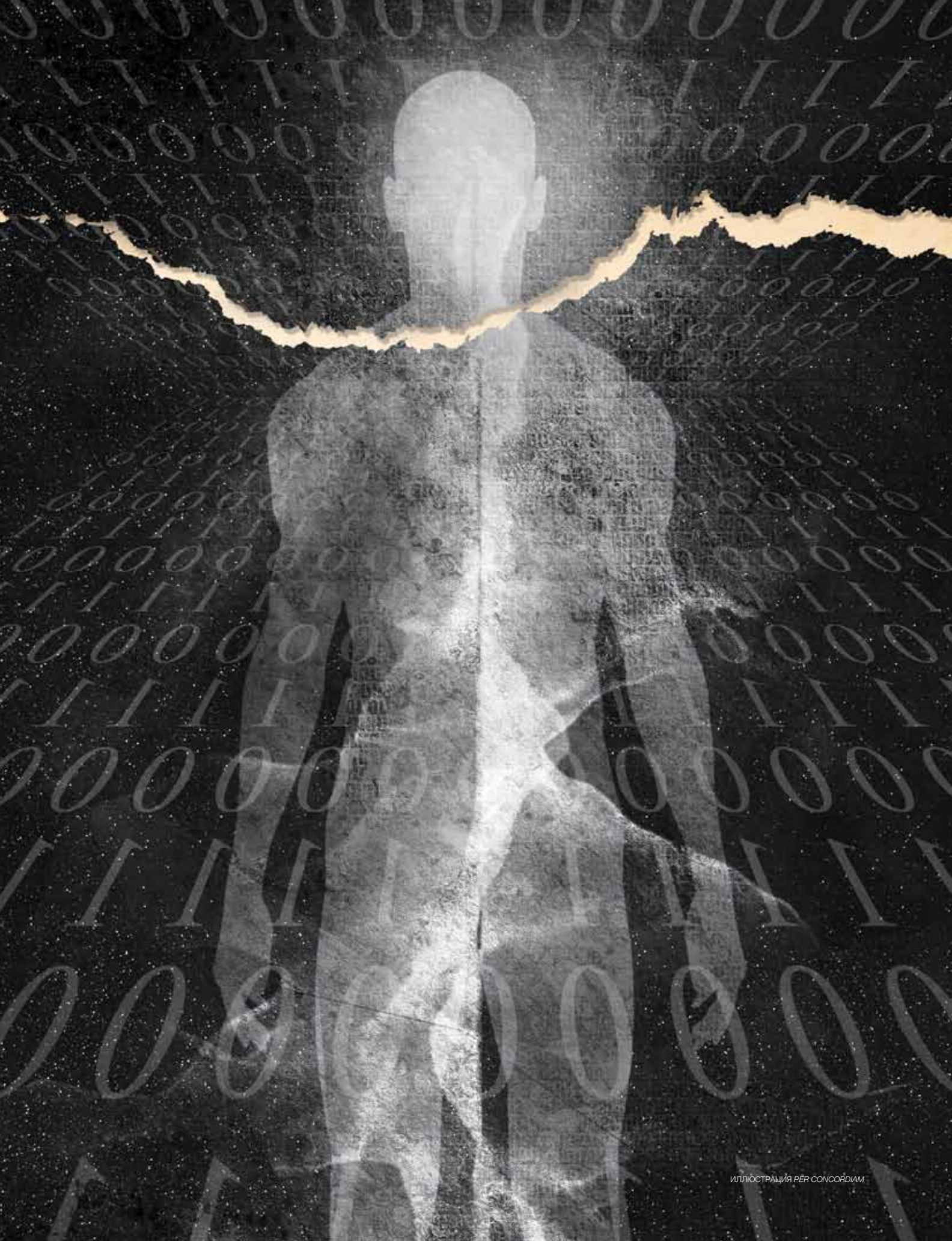


Иллюстрация PER CONCORDIAM

Предотвращение хакерских атак

Преступники орудуют компьютерами как дешевым и анонимным оружием

Кеннет Гирс
Служба уголовных расследований Военно-морских сил США

Интернет изменил почти все аспекты жизни человека, в том числе приемы ведения войны. Сегодня каждый политический и военный конфликт имеет кибернетическое измерение, величина и значение которых трудно предсказуемы.

Компьютеры и компьютерные сети предоставляют новое средство доставки, которое позволяет увеличить скорость распространения, область поражения и значение угроз национальной безопасности. Непрерывное развитие в области информационных технологий далеко опережает как законодательство в этой сфере, так и развитие кибернетической обороны. Повсеместное распространение Интернета и его способность усиливать эффект от любого события могут привести к тому, что сражения, разворачивающиеся в Интернете, будут казаться более важными, чем события, происходящие на земле.

Однако неосязаемая природа кибернетического пространства может сделать оценку победы, поражения и боевых повреждений крайне субъективным делом. Даже определить, имела ли место в отношении тебя кибернетическая атака, может быть проблемой.

Эксперты в области национальной безопасности испытывают трудности с осмыслением всех аспектов понятия кибернетического конфликта по целому ряду причин, в том числе из-за незнания его технических основ, из-за раздуваемой СМИ паранойи и из-за желания успеть воспользоваться высоким коэффициентом окупаемости инвестиций в хакинг.

Автор надеется внести посильный вклад в обсуждение стратегии и тактики кибернетической обороны, дав четкие формулировки основных понятий и определений, относящихся к кибер-войне.

История

С течением времени становится все сложнее и сложнее дать определение тому, что военные называют «полем боя». Обычно технологические достижения являются эволюционными, но они могут быть и революционными: например, когда артиллерийские снаряды сделали возможным воздействие на противника за линией фронта, а ракеты и самолеты – за пределами государственных границ. Сегодня кибернетические атаки могут быть направлены на политических руководителей, военные системы и обычных граждан в любой точке планеты, в мирное или военное время, к тому же обеспечивая анонимность атакующего.

Сегодня каждый политический и военный конфликт имеет кибернетическое измерение, величина и значение которых трудно предсказуемы.

В 1965 году Гордон Мур верно предсказал, что количество транзисторов в компьютерном чипе будет удваиваться каждые два года. Аналогичный рост наблюдается практически во всех аспектах информационных технологий, включая практическую доступность криптографии, дружественных к пользователю хакерских инструментов и разведки на основе открытых интернет-источников.

Сегодня политические и военные стратеги для достижения своих целей вовсю пользуются компьютерами, базами данных и связывающими их сетями. Уже в начале 1980-х годов это явление было известно в Советском Союзе как «военно-технологическая революция». А после войны в Заливе 1991 года придуманное в Пентагоне понятие «Революция в военном деле» стало практически бытовым термином.

В настоящее время кибернетическое пространство в качестве поля боя благоприятствует атакующему, что контрастирует с нашим традиционным пониманием военных действий, в рамках которого обороняющиеся обычно имеют существенное «домашнее» преимущество. Более того, взаимная досягаемость противников перестает быть важной, так как в киберпространстве каждый приходится друг другу соседом. И, наконец, практически не существует морально-этического запрета на компьютерное хакерство, ибо оно главным образом заключается во взаимодействии с программным кодом – и по этой причине не воспринимается как связанное с человеческими страданиями.

Несмотря на все эти преимущества, которыми обладает атакующая сторона, многие аналитики продолжают скептически относиться к серьезности кибернетических угроз. Одна из причин в том, что реальный результат кибернетической атаки вовсе не гарантирован. Тактические победы в кибернетической войне состоят в успешном изменении битов – также известных как «нули и единицы» – внутри компьютеров. После этого атакующий должен ждать, чтобы увидеть, приведет ли такая победа к ожидаемому реальному эффекту.

Мотивация хакеров

Эксперты называют пять основных причин хакинга:

Уязвимость. Недостатки и слабые места интернет-протоколов позволяют хакерам скрытно читать, удалять или изменять информацию, хранящуюся на компьютерах или перемещающуюся между ними. Стремительное распространение интернет-технологий приводит к тому, что обороняющиеся не успевают быть в курсе всех новейших методов атакующих. Каждый месяц в так называемый «тезаурус уязвимостей» (Common Vulnerabilities and Exposures, CVE) добавляется около ста новых пунктов. Одним словом, хакерам доступно больше путей проникновения в компьютерную сеть, чем ее системные администраторы могут защитить.

Коэффициент окупаемости инвестиций. Это относится к правительству, гражданскому обществу и отдельным индивидам. Цели хакера не требуют пояснений: это кража научно-исследовательских и инженерно-конструкторских данных, перехват секретной информации, а также пропаганда в рядах противника. Прелесть компьютерного хакинга заключается в том факте, что все это можно попытаться осуществить, понеся лишь малую часть расходов (и рисков), присущих любой другой стратегии сбора или изменения информации.

Неадекватность кибернетической обороны. Безопасность компьютерных сетей все еще является

АГЕНТСТВО ФРАНС-ПРЕСС

Компьютерный хакер, известный как MafiaBoy, обвиняемый в создании сбоев в работе сети Интернет, покидает здание суда после завершения судебного процесса над ним, проходившего в 2001 году в Монреале.

АГЕНТСТВО ФРАНС-ПРЕСС

Мужчина входит в хорошо охраняемый дата-центр Pionen шведского интернет-провайдера Bahnhof, расположенный в Стокгольме. Дата-центр Pionen, расположенный под стокгольмским парком Витаберг, в подземном ядерном бункере времен Холодной войны, является одним из самых защищенных в мире.

не до конца сформировавшейся дисциплиной. Традиционные навыки в области обеспечения безопасности приносят минимальную пользу в кибернетической войне; к тому же сложно нанять и удержать сотрудников, обладающих техническими навыками, пользующимися спросом на рынке труда. И без того сложные расследования компьютерных преступлений еще более осложняются международным характером интернета. К тому же, в случае кибернетических операций, поддерживаемых на государственном уровне, речи о сотрудничестве между правоохранительными органами различных стран, естественно, не идет.

Правдоподобное отрицание. Напоминающая лабиринт архитектура интернета обеспечивает кибернетическому атакующему высокую степень анонимности. Толковые хакеры направляют свои атаки через страны, с которыми правительство страны-жертвы не имеет хороших дипломатических отношений или с правоохранительными органами которых у страны-жертвы не налажено сотрудничество. Даже успешные расследования компьютерных преступлений зачастую приводят лишь к очередному взломанному компьютеру. Сегодня правительства стоят перед перспективой проиграть кибернетический конфликт, даже не узнав личности противника.

Усиление влияния негосударственных игроков. Эра интернета привела к значительному увеличению числа игроков на мировой арене. Правительства хотели бы иметь монополию на международные конфликты, однако глобализация и интернет значительно повысили возможности каждого человека следить за происходящими в мире событиями и обеспечили мощное средство воздействия на них. Сегодня транснациональные субкультуры сливаются в Сети, оказывают влияние на множество политических задач и никому не подчиняются. Будущее ставит перед мировыми лидерами проблему: смогут ли граждане их собственных стран вывести из-под контроля деликатные проблемы международной дипломатии.

Мишени хакеров

Существует три основных вида кибернетических атак, а все остальные являются производными от них:

Конфиденциальность. Сюда входит любой несанкционированный сбор информации, включая так называемый «анализ трафика», в котором атакующий делает выводы о содержании сообщений, основываясь лишь на выявленных закономерностях в обмене содержащими эти сообщения данными. Так как сегодня в мире связь компьютерных сетей намного превышает их безопасность, для хакеров не представляет труда воровать гигантские объемы информации.

Кибернетический терроризм и кибернетическая война могут быть делом нашего будущего, но мы уже живем в золотом веке кибернетического шпионажа. Наиболее известным на настоящий момент случаем является «дело GhostNet», расследовавшееся организацией Information Warfare Monitor: была выявлена шпионская компьютерная сеть, состоящая из более тысячи скомпрометированных компьютеров, расположенных в 103 странах и занимавшаяся сбором дипломатической, политической, экономической и военной информации.

Целостность. Сюда входит несанкционированная модификация информации или информационных ресурсов, таких как базы данных. Такие атаки могут включать «саботаж» данных в преступных, политических или военных целях. Например, кибер-преступники зашифровали данные на жестком диске жертвы и требуют деньги в обмен на ключ расшифрования; правительства, осуществляющие цензуру поисковой системы Google, возвращают конечному пользователю лишь часть выданных поисковой системой результатов.

АГЕНТСТВО ФРАНС-ПРЕСС

АГЕНТСТВО ФРАНС-ПРЕСС

Шотландскому хакеру Гэри Мак-Киннону грозит экстрадиция в США на основании законов по борьбе с терроризмом, так как в 2001 году он взломал военные компьютеры США. Ему может грозить до 70 лет тюрьмы.

Предполагаемого боевика Всемирного исламского медиа-фронта ведут в зал суда в Вене в августе 2009 года. Он был приговорен к четырем годам тюремного заключения за создание исламского видео с угрозами, впоследствии распространенного через интернет.

Доступность. Здесь целью является помешать легитимным пользователям получить доступ к системе или к данным, необходимым им для выполнения определенных задач. Атаки такого рода часто называют DoS-атаками (Denial-of-service attack, атака типа «отказ в обслуживании»). Для таких атак используется широкий спектр вредоносных программ, атаки при помощи сетевого трафика и физические атаки на: компьютеры, базы данных и связывающие их сети.

В 2001 году хакер MafiaBoy – 15-летний школьник из Монреаля – провел успешную DoS-атаку против нескольких крупнейших сетевых компаний, финансовый ущерб от которой составил, по всей видимости, более одного миллиарда долларов.

Задачи хакеров

Кибернетическая атака не является самоцелью, это лишь замечательное средство для достижения широкого спектра целей, разнообразие которых ограничено, в основном, воображением атакующей стороны.

Шпионаж. Каждый день анонимные компьютерные хакеры крадут огромные объемы компьютерных данных и сетевых сообщений. В сущности, опустошительные операции по сбору разведданных – даже по отношению к совершенно секретной политической и военной переписке – можно проводить из любой точки земного шара.

Пропаганда. Она дешева и эффективна, а поэтому зачастую является самой легко осуществимой и мощной формой атаки. Цифровую информацию в виде текстов или изображений – независимо от ее правдивости – можно моментально скопировать и переслать в любую точку планеты, даже в далекий тыл противника. А провокационная информация, подвергшаяся цензуре, может секундой позже появиться в другом месте Сети.

Отказ в обслуживании (DoS). Целью является помешать использованию данных или компьютеров легитимными пользователями. Наиболее распространенной тактикой является атака целевой компьютерной системы потоком бессмысленных запросов, чтобы она не имела возможности отвечать на реальные запросы услуг или информации. Другие виды DoS-атак включают физическое повреждение аппаратных средств и использование электромагнитных помех с целью повреждения неэкранированной электроники путем скачков силы тока или напряжения.

Модификация данных. Успешная атака на сохранность секретных данных может привести к тому, что легитимные пользователи (люди или компьютеры) будут принимать важные решения на основе преднамеренно искаженной информации. Такие атаки приводят к различным последствиям: от искажения внешнего вида веб-сайта (которое часто называют «электронным граффити», но которое, тем не менее, может при этом содержать пропаганду или дезинформацию) до повреждения современных систем вооружения.

Воздействие на инфраструктуру. Все больше и больше национальных объектов критической инфраструктуры подключено к интернету. Однако системы безопасности на таких объектах могут быть не очень надежными, так как от них может требоваться немедленная реакция, а аппаратная составляющая может не обладать достаточной для этого вычислительной мощностью. Экспертам в области национальной безопасности следует обратить особое внимание на системы генерации и распределения электричества, так как у электричества нет заменителя и все остальные объекты инфраструктуры зависят от него. И, наконец, важно отметить, что многие объекты критической инфраструктуры находятся в частных руках.

Кибернетические атаки во время войны

В будущем конечная цель войны – победа – останется неизменной; советы Сунь Цзы и Клаузевица не утратят своего значения. Однако в кибернетическом пространстве применима совершенно другая тактика ведения войны, и в случае войны между крупными мировыми державами первой жертвой конфликта может стать сам интернет.

Во время большой войны будут две основных категории кибернетических атак:

Вооруженные силы противника. Эти атаки будут проводится в качестве составляющей части общих усилий, направленного на выведение из строя вооружения противника и на нарушение работы его военных систем командования и управления.

В 1997 году Министерство обороны США провело широкомасштабные учения по противодействию кибернетическим атакам под названием «Eligible Receiver».

Игра завершилась успешно. По словам Джеймса Адамса (журнал «Foreign Affairs»), игравшие роль северокорейских хакеров 35 сотрудников Агентства национальной безопасности, использовав различные тактические приемы ведения информационной кибернетической войны, смогли «заразить человеческую систему командования и управления парализующим ее работу уровнем недоверия. … В результате в вертикали управления никто, от президента и до низовых структур, не мог ничему верить».

В 2008 году неизвестные хакеры получили доступ как к несекретным, так и к секретным компьютерам Центрального командования вооруженных сил США – структуры, отвечающей за управление войсками в обеих войнах, которые сейчас ведут США. Эта атака так встревожила Пентагон, что Председатель Объединенного комитета начальников штабов Майкл Маллен лично докладывал о ней Джорджу Бушу.

Можно с уверенностью предположить, что в случае войны между крупными державами описанные выше атаки померкнут в сравнении со сложностью и масштабом тех кибернетических средств и тактических приемов, которые держатся правительствами про запас на то время, когда под угрозой будет их национальная безопасность.

Гражданская инфраструктура противника. Эти атаки будут нацелены на способность и желание противника вести войну в течение длительного периода времени; их объектами могут стать финансовый сектор, промышленность и моральных дух населения противника.

Одним из наиболее эффективных способов ослабить множество подобных целей второго эшелона является нарушение генерации и распределения электричества. В мае 2009 года президент Барак Обама сделал неожиданное заявление: «Кибернетические злоумышленники уже пытались проникнуть в наши сети электроснабжения. … В других странах целые города остаются без света из-за кибернетических атак». Считается, что эти атаки имели место в Бразилии в 2005 и 2007 годах, что они затронули миллионы гражданских лиц и что источник этих атак до сих пор неизвестен.

Говоря о гипотетических кибернетических атаках против финансового сектора, бывший Директор Национальной разведки США Майк МакКоннелл сказал, что наибольшее беспокойство у него вызывает не сама кража денег, а атака на целостность финансовой системы как таковой, имеющая целью уничтожить веру общества в безопасность финансовой системы и в ликвидность денежной массы.

Сегодня военные могут воспользоваться всеобщей подключенностью к Сети для проведения широкого спектра кибернетических атак против объектов критической инфраструктуры противника, воздействуя на последнего далеко за линией фронта.

Взгляд в будущее

Интернет изменил природу боевых действий. Компьютеры являются одновременно и оружием, и мишенью для нападения. Как и в случае с терроризмом, хакеры являются предметом ажиотажного интереса СМИ. И как и в случае с оружием массового уничтожения, сложно осуществить возмездие в ответ на асимметричную атаку.

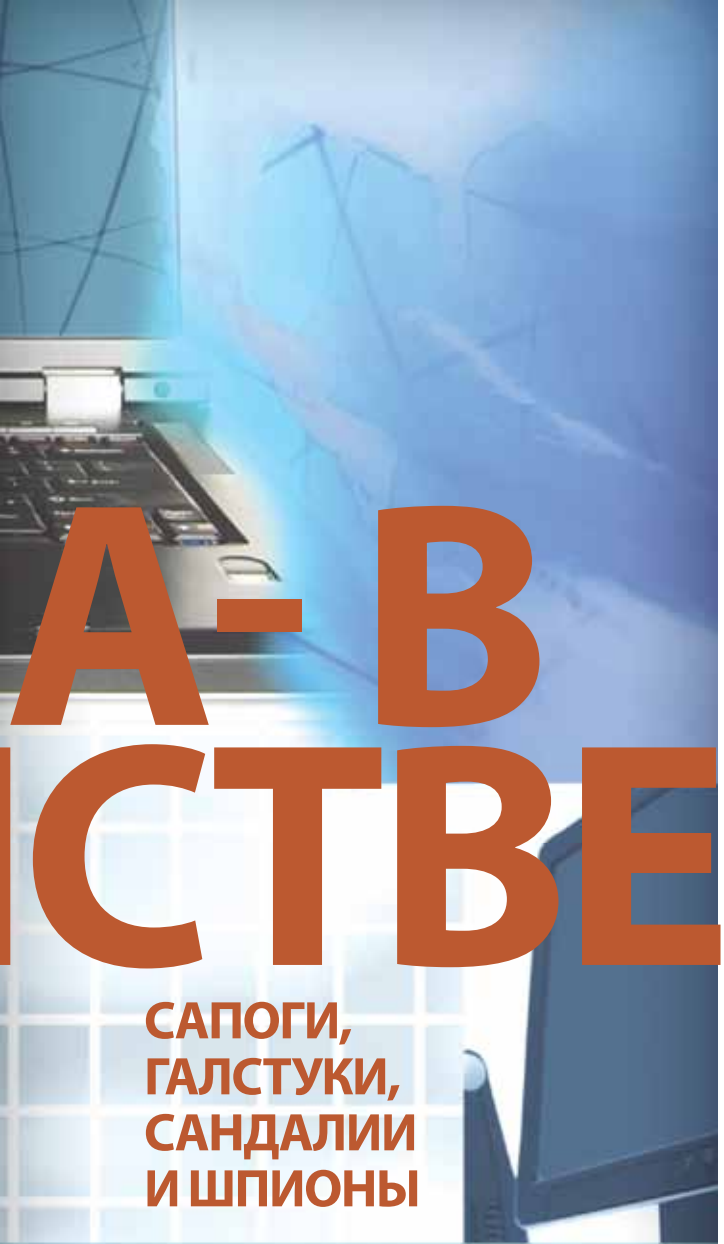
в случае войны между крупными мировыми державами первой жертвой конфликта может стать сам интернет.

С учетом всего вышесказанного, кибернетическая война благоприятствует странам с развитой отраслью информационной технологии, однако интернет – мощное оружие, дающее более слабой стороне возможность атаковать более сильного, в традиционном смысле, противника. Также следует иметь в виду, что страны, сильно зависящие от интернета, пострадают больше других в случае, если произойдет сбой в работе Сети.

С точки зрения обороны, странам следует развивать технологии, способные уменьшить два ключевых преимущества хакеров: трудности с определением личности атакующего и высокий уровень асимметрии. Зачастую анонимная природа хакинга и его крайне высокий коэффициент окупаемости инвестиций могут сделать неэффективными традиционные меры по минимизации рисков, такие как устрашение и контроль над вооружениями.

На данном историческом этапе многие правительства могут почувствовать себя вынужденными готовиться к кибернетической войне, видя в ней не только средство проецирования своей силы, но и единственное средство защиты своего присутствия в кибернетическом пространстве. □

СИЛ
ЕДИН



А-В ЦТВЕ

САПОГИ, ГАЛСТУКИ, САНДАЛИИ И ШПИОНЫ

ДЖУПИТЕР

Опыт, наработанный в результате Всестороннего Подхода к Национальной Кибербезопасности

Александр Климбург,
Австрийский институт иностранных дел

Определяющим элементом национальной кибернетической безопасности является Важная роль неправительственных структур. Более десятилетия многие правительства поддерживали программы защиты ключевой инфраструктуры (ЗКИ) с целью содействия сотрудничеству между правительством и ведущими компаниями частного сектора, особенно, в сфере кибернетической безопасности. Результаты оказались противоречивыми, и становится все более понятно, что многостороннее вовлечение неправительственных структур возможно только в рамках отак называемого «Общенационального» подхода (ОП) — метода межведомственного сотрудничества.

Важная роль частного сектора и гражданского общества в сфере национальной кибернетической безопасности очевидна. Частный сектор отвечает за практически все программное и аппаратное обеспечение, используемое при осуществлении кибернетических атак, обслуживает большую часть сетевой инфраструктуры, на которой проводятся эти атаки, и зачастую владеет объектами жизнеобеспечения, против которых совершаются эти нападения. Более того, структуры гражданского общества, в отличие от частного сектора, доминируют в кибернетическом пространстве, определяя параметры программ (т.е. протоколы ПО) кибернетической территории, равно как и исполняя, исследуя и открыто спекулируя на кибернетических атаках. Все вместе эти неправительственные структуры составляют основу того, что называется «национальной» кибернетической безопасностью. В большинстве национальных программ ЗКИ их учитывают только частично.

Некоторые критики, особенно в США, обеспокоены тем, что Общенациональный подход уделяет вооруженным силам все большую роль, как это недавно произошло с общественной деятельностью только что основанного Кибернетического командования ВС США. В этом есть доля правды, однако, данная критика угрожает срывом куда более важного вопроса, чем участие вооруженных сил в сфере деятельности преимущественно гражданского сектора. Все структуры, имеющие отношение к кибернетическому пространству, как внутри, так и вне правительства, должны в большей степени участвовать в вопросах кибернетической безопасности.

Разница между программами ЗКИ и ОП заключается, прежде всего, в их масштабности. Программы ЗКИ (применимо к вопросам кибернетической безопасности) направлены на отражение отдельных нападений, а кибернетическая безопасность в Общенациональном больше

направлена на поиск средств борьбы с используемыми в ходе нападений методами, например, улучшение качества ПО с целью предотвращения ошибок системы, которые можно использовать для проведения кибернетической атаки, или решение вопроса сохранения данных и их обмен. Также кибернетическая безопасность по ОП должна учитывать возможные «катастрофические» кибернетические нападения на национальную инфраструктуру, т.е. нападения, которые могут быть совершены в контексте кибернетической войны. На самом деле, враждебные действия в кибернетическом пространстве могут финансироваться государствами или даже являться первым шагом к началу кибернетической войны. Поэтому, чтобы быть готовым к кибернетичесой войне, необходимо внимательно наблюдать за вызывающей подозрение деятельностью, которая может оказаться кибернетическим преступлением или терактом.

В то время как в кибернетической безопасности нет должного определения Общенационального подхода, подобные инициативы были успешно внедрены рядом стран. В контексте так называемых стратегий «Предотвращение конфликта» или «Уязвимые государства», которые, в понимании вооруженных сил, включают в себя операции по стабилизации, подобно тем, что проходят в Афганистане и Ираке, Общенациональный подход применяется уже много лет, хотя и не всегда под одним и тем же названием.

Всесторонний подход НАТО является еще одним примером использования данного подхода на практике. Существует также множество государственных доктрин, особенно известные из которых, к примеру, доктрины Соединенного Королевства, Нидерландов, Канады, Дании и Финляндии. Сотрудничество структур обороны, дипломатии и развития всегда является главным в этих доктринах. Для их осуществления требуется тесное сотрудничество вооруженных сил, политологов, гражданского общества и разведсообщества – или «сапог, галстуков, сандалий и шпионов», - чтобы найти общие решения не только на оперативном уровне в соответствующей области деятельности, но также на политическом уровне в соответствующей столице государства.

Общенациональный подход связан с объединенными усилиями государства (всего правительства) и негосударственных структур (предприятий, гражданского общества), направленными на достижение общей цели. В стратегии «Уязвимые государства» данная цель обычно представляется как стабилизация региона или страны. В кибернетической безопасности данная цель, как правило, связана со снижением уязвимости национальных сетей и объектов жизнеобеспечения. В ближайшие три-пять лет предстоит решить целый ряд вопросов, связанных с кибернетической безопасностью. Краткий перечень «горячих» вопросов включает в себя сохранение данных и их секретность, ответственность компаний-производителей ПО, привлечение граждан государств к внедрению базовой кибернетической безопасности,

РЕЙТЕР

На снимке показана штаб-квартира коммуникаций правительства Великобритании в Челтенхеме. Терроризм и кибернетическая безопасность занимают центральное место в национальной стратегии безопасности страны.

сотрудничество владельцев объектов инфраструктуры жизнеобеспечения и, прежде всего, обмен информацией между правительственными и неправительственными структурами.

Чтобы не «изобретать велосипед» в области кибернетической безопасности, рекомендуется учиться на опыте работы в рамках Общенационального подхода. По сути, в основе ОП – процесс, а все процессы в значительной степени воспроизводимы. Несмотря на кажущееся отсутствие общности между операциями по обеспечению стабильности и кибернетической безопасностью, их объединяет один значительный общий фактор: важность работы с неправительственными структурами.

В последние несколько лет по поручению правительства Австрийский институт иностранных дел проводил исследования Общенациональных подходов разных государств. Частично на основании этого исследования институт разрабатывает новый Всесторонний подход к международным операциями (известный как АЕК – от нем. «Auslandseinsatzkonzept») и Австрийскаую программу защиты объектов жизнеобеспечения (АПЗОЖ). Хотя полный список «наработанного опыта» может занять много страниц, можно сделать общие выводы относительно Общенационального подхода, особенно в отношении программ ЗКИ.

«Сверху вниз» или «снизу вверх»

Необходимость того, чтобы высшее руководство начало процесс как в сфере предотвращения конфликта, так и в сфере кибернетической безопасности, является приоритетной. Хотя это кажется очевидным, серьезные культурные барьеры, с которыми часто можно столкнуться в ОП, означают, что реальная заинтересованность на высшем уровне является первостепенной. Различные организации могут иметь укоренившиеся интересы, которые, на первый взгляд, кажутся неизменными. Только используя подход «сверху вниз», можно надеяться на преодоление этих препятствий, хотя действия на основании опыта оперативной базы могут оказаться полезными. В самом деле, иногда лучший подход – это подход «снизу вверх» («работа с широкими кругами») на основании ранее созданных сетей связи на уровне рабочих групп.

РЕЙТЕР

Специалист по сетевой обороне работает в Центре безопасности и сетевых операций космического командования ВВС США на авиабазе ВВС США «Петерсон», расположенной в штате Колорадо (США). Ответственные за планирование национальной безопасности предлагают подобным же образом защитить объекты жизнеобеспечения, такие как электросети, коммуникации и финансовые сети, от кибернетических мародеров.

Это особенно важно, когда целью является обмен информацией. Возможно, самый важный инструмент в кибернетической безопасности - обмен информацией подразумевает обмен данными высокой чувствительности, в основном, о случившихся кибернетических атаках и их последствиях. В большинстве стран Европы эти информационные обмены в общем часто называются Государственно-частными партнерствами (ГЧП), хотя подобные обмены могут также происходить между правительственными организациями и даже частными предприятиями напрямую. В США наиболее распространенная форма кибернетического ГЧП известна как ЦОАИ (Центры обмена и анализа информации), которые содержаться для определенных промышленных вертикалей, таких, как энергетика, вода, финансы и др. Хотя ЦОАИ вносят значительный вклад в кибернетическую безопасность США, первые годы их существования были проблематичными, частично, за счет того, что не имелось личной заинтересованности и участия в верхних эшелонах отрасли и практически не было попыток выйти на связь с уже существующими программами. Подобная модель в Великобритании, которая называется WARP, имела больший успех за счет поддержки бизнеса и правительства.

Важно отметить, что, с точки зрения военных кибернетиков, некоторые важнейшие сведения накапливаются именно этими группами. Для получения доступа к этой информации необходимо участвовать в процессе обмена. Иными словами, сведениями разведки нужно делиться и с этими неправительственными структурами. Проверенным инструментом в этом информационном обмене является протокол «Светофор» , хотя при этом многим правительственным структурам часто необходимо юридически менять способ обращения с конфиденциальными материалами.

Терпеливо строить доверительные отношения

В случаях, когда стороны не знакомы друг с другом и имеют ряд серьезных предубеждений, важно поближе познакомиться. Это особенно применимо в случае группы «сапоги - сандалии», структур развития и вооруженных сил, сторонников защиты данных и сотрудников служб государственной безопасности.

Личный опыт показывает, что первые встречи, казалось бы, проходят неудачно, но обе стороны почти всегда соглашаются продолжать диалог. Последующие встречи значительно способствуют взаимному культурному пониманию. Это главное в создании доверительных отношений, и здесь требуется терпение. Исходя

из опыта, также крайне рекомендуется, чтобы группа состояла из одних и тех же лиц, присутствующих на каждой встрече.

Также важно понимать, что результатом ОП не может быть «изменение ключевой идеологии». Определенные понятия, важные для деловых структур и структур гражданского общества, такие как защита интеллектуальной собственности или сохранение «гуманитарного пространства», на первый взгляд, расходятся с требованиями правительственных структур. Тем не менее, личные заблуждения могут измениться, и часто это необходимо, если правительственные и неправительственные структуры будут работать вместе.

Очень успешная швейцарская организация MELANI (правительственный центр кибернетической безопасности, ведущая работу в сфере защиты объектов жизнеобеспечения) в момент своего основания насчитывала всего с десяток клиентов в частном секторе. Частный сектор волновали проблемы, решить которые казалось невозможным. Эти проблемы включали в себя защиту данных и сомнения частного сектора относительно общей компетентности государственного сектора. Спустя четыре года MELANI насчитывает несколько сотен клиентов, включая большинство ведущих международных банков, и имеет прекрасную репутацию как у себя в стране, так и за рубежом. Компания годами завоевывала доверие клиентов. Ее работа оказалась выгодной не только для частного сектора. В результате развития этой широкой сети доверия швейцарские военные и гражданские органы кибернетической безопасности получают сведения одной из лучших кибернетических разведок.

«Честный брокер»

Действия ОП невозможны в социально-политическом вакууме и отражают общее восприятие относительной политической власти участвующих структур. Часто, если не всегда, государственный сектор воспринимается как самый сильный политический игрок за столом. Обычно именно по инициативе государства создается процесс ОП. Остальные участники могут быть изначально менее убеждены в полезности самого процесса, и будут будут считать, что большинство его аспектов (включая участие) зависит от переговоров в других областях.

Как у инициатора, у государства есть две возможности подойти к этому деликатному вопросу. Можно повести себя как «primus-inter-pares» (первый среди равных). В таком случае, государство напрямую пытается представить свои интересы за столом, равно как и управлять процессом. Преимущество государства в том, что оно может напрямую взаимодействовать с другими структурами, и считает результат более важным, чем процесс. Недостаток же заключается в том, что государство должно представлять собой совершенно единый фронт (т.е., если присутствует более чем одна правительственная структура, иерархия между структурами должна быть ясна всем участникам).

ДЖУПИТЕР

Процесс может также превратиться в хитроумные политические игры государства с отдельными негосударственными структурами, что не позволит добиться институционального участия со стороны этих структур. Страны, взявшие на себя роль «primus-inter-pares», - это, прежде всего, США, Великобритания и Австралия. В каждом случае одно правительственное ведомство или департамент уполномочен вести эти переговоры. Например, в Великобритании эта ответственность вменена Центру защиты национальной инфраструктуры, или ЦЗНИ.

Второй возможный подход – посредничество «честного брокера». Такой посредник напрямую не заинтересован в исходе переговоров и, таким образом, занимается только процессом. Часто государство доверяет эту задачу негосударственной структуре, такой как научно-исследовательский центр, который, таким образом, занимает смешанную позицию в процессе.

Преимущество данного подхода заключается в том, что, разделяя процесс и результат, процесс становится более беспристрастным, возможно, более благоприятным для создания «общенационального» настроения в структурах. Также это особенно полезно, когда ни одна из правительственных структур, представленных за столом переговоров, не желает представлять государство. Недостаток этого подхода заключается в том, что посредник может завысить важность процесса над результатом, таким образом, сокращая возможность положительных побочных результатов, как, например, новые программы. При этом снижается объем частных переговоров, поскольку процесс имеет более коллективную природу. Пример данного подхода – Национальный институт по борьбе с кибернетической преступностью (НИБКП) в Нидерландах.

Работает ли «стратегия объединения»?

Прозрачность и вовлеченность имеют свои преимущества, но также и свои недостатки. В практических примерах наблюдаются огромные различия между подходом с участием малой, конфиденциальной группы избранных и объединяющим подходом. Есть доказательства в пользу того, что лучше начинать с малого и расти к большему.

Что касается кибернетической безопасности, существуют четкие показатели того, что подход с задействованием малых групп имеет большие шансы на успех. Например, как недавно заявил замминистра обороны США Уильям Линн, Кибернетическое командование ВС США разработало несколько новых мер безопасности, таких как внедрение автоматизированной активной обороны от кибернетических нападений с целью защиты промышленной базы. Эти результаты стали возможны, в основном, благодаря тесному сотрудничеству между командованием и некоторыми оборонными подрядчиками.

На менее крупном, тактическом, уровне часто встречается общее понимание того, что малые группы эффективнее обмениваются информацией, чем более крупные. Например, и +ЦЗНИ, и НИБКП работают с группами не более 24 человек.

Тем не менее, ОП требует гораздо более широкого участия, чем имеющиеся на сегодня традиционные программы ЗКИ. В отличие от программ ЗКИ, ОП должен приводить к гораздо более обширным изменениям в политике, нежели чем вышеописанные «оперативные меры». Например, как должно правительство мотивировать производителей программного обеспечения более ответственно подходить к защищенности их продуктов, учитывая, что большинство кибернетических атак становится возможным из-за ошибок в их программах? Как оно может убедить большее количество частных предприятий внести свою лепту в защиту национальной безопасности, предоставив имеющиеся у них данные? Эти вопросы не решить в малых засекреченных группах; для их решения требуются широкие дискуссии и политическая поддержка, даже если сначала полезно проконсультироваться по ним с малой группой.

Этот подход уже доказал свою продуктивность в предотвращении конфликтов. В одной рассмотренной нами стране гражданские лица и правительство начали конфиденциальный процесс консультаций, получивший название известного в стране пляжного отеля. Одним из результатов стала молчаливая гражданская поддержка военной кампании в Афганистане. Еще одним результатом стала широкая общественная дискуссия по вопросам развития и помощи в поддержку развития, а также о том, каким образом ее лучше всего задействовать. В результате этого общественного дискурса, даже в свете недавнего экономического кризиса, бюджеты гуманитарной помощи и помощи развития остались неприкосновенными. Очевидно, что общественная дискуссия, столь полезная для сообщества в целом, была возможна только благодаря предварительной работе малых групп над созданием доверительных отношений и обменом информацией и опытом.

Помимо приведенного выше наработанного опыта, включая многочисленные препятствия, получены и иные наработки. Однако именно вышеупомянутое иллюстрирует, что подход WoN, действительно, является процессом и, как и все процессы, должен быть вопроизводим в разных обстоятельствах. «Ботинки, галстуки, сандалии и шпионы» не всегда представляют одни и те же структуры. Например, термин «сандалии» может относится как к разработчикам, так и блоггерам. Частный сектор, также, имеет решающее значение в программах CIP, тогда как в предотвращении конфликтов главной негосударственной группой являются неправительственные организации. Тем не менее, в обоих случаях, главное – обширное сотрудничество традиционно антагонистически настроенных групп.

В целом, процесс WoN представляет собой изменение парадигмы о том, как политика безопасности может проводиться в либеральных демократиях, и новая парадигма основана на доверии, общих интересах и распределении власти. □

Как защитить

Новак Джорджиевич, ВВС Сербии

кибернетическое пространство

Международное право должно регулировать борьбу с угрозами безопасности, исходящими из Интернета

ИЛЛЮСТРАЦИЯ *PER CONCORDIAM*

Современные угрозы безопасности характеризуются, помимо прочего, асимметричностью и гибкостью. Однако, в современном мире угрозы безопасности выходят за пределы материальной сферы, физической безопасности и свободы отдельного лица и вторгаются в экономическую, интеллектуальную и частную сферы жизни. Мы не только ведем деятельность и выстраиваем отношения в материальной реальности, но и общаемся, обмениваемся информацией, выполняем различные задания, развлекаемся и совершаем покупки в параллельной виртуальной реальности, пользуясь услугами глобальной сети — Интернета. В информационном облаке Интернета мы оставляем следы своей деятельности — следы, соединяющие нас с другими людьми, ведомствами, компаниями и организациями. Оставляя после себя эту информацию, мы непреднамеренно рассказываем о себе больше, чем сами бы хотели.

Такие следы являются полезной информацией для кибернетических преступников. Пользуясь этой и другой информацией, кибернетические преступления могут достичь самых невероятных целей. Помимо частных лиц, которые часто становятся жертвами их нападений, киберпреступники атакуют сайты, информационные порталы, электронные почтовые системы, социальные сети, корпоративные сети или сети правительственных и неправительственных организаций и даже других преступников.

Но что такое кибернетическая преступность? Попросту говоря, это незаконное использование компьютеров и Интернета или преступление, совершенное с использованием компьютеров или Интернета. Это определение можно расширить, включив в него и другие телекоммуникационные устройства, такие как мобильные телефоны, карманные персональные компьютеры и прочие электронные устройства, устанавливающие соединение с другими устройствами.

Мотивы кибернетической преступности

Часто бывает трудно понять, что движет кибернетическими преступниками. Дать хорошую классификацию мотивов — непростая задача, но некоторые из самых распространенных перечислены ниже:

- Политические/религиозные (распространение политических, религиозных или иных идей, осуществление политических, религиозных и иных целей, возмездие за политические и иные действия и т.д.)
- Материальная выгода
- Идеализм (попытка доказать свои умение и способности, не рассчитывая на материальную выгоду или иное вознаграждение)
- Любознательность, тяга к приключениям (в основном, это новички, которые еще не занимаются серьезной преступной деятельностью - «взломщики кодов», «хакеры», «технари» - искатели легкого заработка или славы, которым не хватает знаний и умения).

Эта неполная классификация помогает нам увидеть, почему пополняются ряды кибернетических преступников. Осознание того, что в Интернете можно пропагандировать политические идеи при помощи незаконных средств, нелегально заработать денег или просто безнаказанно взломать сайт, толкает людей на преступления — и, по сути, остановить их могут только личные нравственные убеждения. Это приводит к выводу, что данный тип преступности будет расти и развиваться. С годами кибернетическая преступность приобретает все больший размах. Но мало того, по некоторым мрачным прогнозам, производство вредоносного программного обеспечения вскоре может превзойти по своему объему производство легального программного обеспечения.

По мнению экспертов, одной из причин распространения этого вида преступности является неблагоприятное сочетание трех факторов: риска, усилий и выгоды. При нынешнем положении вещей злоумышленники имеют дело с очень небольшим риском, от них требуются скромные усилия, а возможная выгода — довольно велика. Если бы удалось изменить это соотношение при помощи продуманной стратегии (высокий риск — умеренные усилия — малая выгода, см. Рис. 1), то есть, ослабить побуждающие стимулы для преступников, тогда возможно было бы существенно снизить уровень кибернетической преступности.

Знай своего врага

Согласно докладу Центра приема жалоб на мошенничество в Интернете (IC3), в 2009 году IC3 получил 336 665 заявлений о мошенничестве по сравнению с 16 883 в 2000 году, то есть почти в 20 раз больше. Финансовые убытки за тот же период увеличились почти в 32 раза. Большинство потерпевших сообщили о потере от 100 до 1 тыс. долларов (36,7%), а почти 87 процентов потерпевших потеряли менее 5 тыс. долларов. Эти данные свидетельствуют о том, что кибернетическая преступность приобретает все больший размах.

Однако всерьез ли мы воспринимаем эту угрозу? Широкие слои общественности имеют смутное представление о кибернетической преступности. В отличие от традиционных форм преступности, она кажется безликой, и неясно, состоят ли криминальные структуры из отдельных лиц, преступных группировок или из тех и других. Личность кибернетического преступника формируется под воздействием особых социальных, технологических, экономических, наследственных и прочих факторов. Теоретически кибернетическим преступником может стать каждый.

Недавно компания «Symantec», занимающаяся разработкой систем компьютерной безопасности, опубликовала результаты исследования, в ходе которого были проанализированы взаимоотношения между кибернетической преступностью и общественным мнением на основе выборки в 7 тыс. респондентов из 14 стран. Согласно результатам исследования, большинство людей ошибочно полагает, будто кибернетическая преступность не является разновидностью организованной преступности, хотя экспертный анализ выявил, что «в настоящее время 90% кибернетических атак являются непосредственным результатом организованной преступности». Иными словами, большинство людей считает, что кибернетическая преступность является деятельностью отдельных лиц, хотя факты говорят о том, что она имеет организованный характер. Это означает, что решение проблемы кибернетической преступности требует организованного, систематического, международного подхода.

Чтобы сформировать адекватные стратегии борьбы с кибернетической преступностью, необходимо понять действие преступных механизмов в материальной сфере (их modus operandi). Для этого лучше всего изучить топологию кибернетической преступности. Киберпреступники часто организуются в небольшие группы, умело использующие программное и аппаратное обеспечение. Однако преступникам, состоящим в одной группе, необязательно физически находиться в одном месте. Они могут действовать из разных городов, регионов, стран и даже с разных континентов. Кроме того, они используют технику, которую можно взять в аренду в любой стране. При помощи Интернета преступники могут осуществлять свою деятельность на удаленной основе.

Отследить деятельность столь аморфных организаций крайне трудно, а еще труднее бороться с ними правовыми методами. В силу своей топологии кибернетическая преступность является феноменом глобальной организованной преступности и представляет все большую угрозу для всех нас. Кибернетическая преступность можно уподобить раку кибернетического организма. Через некоторое время после устранения одной проблемы обычно возникает новая в другом месте. Сдержать кибернетическую преступность так же сложно, как и рост раковых клеток.

Одного щита недостаточно

Существует ли стратегия контроля темпов роста и масштаба кибернетической преступности? Почему нынешние методы борьбы с кибернетической преступностью приносят лишь скромные результаты?

Методы борьбы с кибернетической преступностью были разработаны на заре компьютерной эры, когда вредоносные программы разносились посредством гибких дисков, а распространение вируса занимало довольно много времени. С появлением сетей темпы распространения вредоносных программ многократно увеличились. Теперь такие программы разносятся почти мгновенно. Единственная преграда между двумя узлами сети — это механизмы компьютерной охраны.

Однако существующие методы защиты являются оборонительными и представляют собой системы ответных мер. Это означает, что они реагируют на появление в компьютере вредоносных программ, распознавая те из них, которые им известны, но бессильны перед изобретательностью киберпреступников. Метод ответной меры означает, что можно бороться с известными угрозами. Сначала выявляется новая угроза, затем создается защитный механизм (обновление программы, удаление зараженных файлов, блокирование определенных действий и т.д.), который, наконец, поступает в распоряжение пользователей как часть общего защитного механизма. Проблема в том, что данный процесс является относительно медленным, поэтому ущерб наносится всегда. Модель безопасности – это «щит», призванный защитить компьютер от злоумышленников. Примерами контроля доступа являются межсетевые защитные экраны, пароли, антивирусные программы и спам-фильтры. Но все это пассивная защита. Без активных механизмов существующие системы безопасности неспособны помешать кибернетическому преступнику нанести ущерб до того, как он войдет в сеть.

Создать активные методы, коренным образом отличающиеся от оборонительных и ответных мер, возможно, но для этого потребуется существенное изменение технологии, на которой основан Интернет. Во-первых, необходимо осознание того, что кибернетическая преступность — это вид социальной деятельности, пронизывающий несколько материальных и виртуальных слоев (см. Рис. 2).

Как социальный индивидум кибернетический преступник - основа криминальной схемы. Человек как таковой скрывается под несколькими защитными слоями — это псевдонимы и аватары, законы страны о неприкосновенности частной жизни, характеристики телекоммуникационного оборудования и программного обеспечения, которые позволяют или не позволяют отслеживать перемещение вредоносных программ в сети.

Сценарий, при котором кибернетическое преступление происходит в одной стране, а преступники находятся в другой, можно назвать «проецированием преступления», когда источник проблем создает проблему не в своей среде, а проецирует ее на расстояние, в среду, которая не может оказать эффективного сопротивления патогенам. В этом заключается фундаментальная стратегия кибернетической преступности, которая позволяет ей существовать и развиваться практически беспрепятственно. Для борьбы с этой стратегией необходимо разработать средства глобального масштаба.

Отпор глобального масштаба

Эффективная активная стратегия против кибернетической преступности подразумевает следующее:

- Единая трактовка киберпреступности с точки зрения международного права.
- Пересмотр телекоммуникационных стандартов (аппаратного и программного обеспечения).
- Переосмысление рамок защиты неприкосновенности

частной жизни.
- Просвещение пользователей (положительная социальная инженерия).
- Международное сотрудничество и координирование в плане выявления, мониторинга и уничтожения преступности.

Важным препятствием на пути борьбы с кибернетической преступностью является несовершенство правовых механизмов. Нормативные акты, принимаемые на государственном и межгосударственном уровне, являются фундаментом, на котором строится глобальный механизм борьбы с кибернетической преступностью. Конечно, борьба с киберпреступностью возможна даже при нынешней модели «каждый сам за себя», но такая модель дорога, малоэффективна и едва ли жизнеспособна. В долгосрочном плане — если не произойдет существенного изменения характера кибернетической преступности — пока каждый из нас будет гоняться за одной пираньей, стая пираний разорвет нас на части.

Пересмотр телекоммуникационных стандартов позволит осуществлять мониторинг информационных потоков, отслеживая источник, маршрут и конечную точку телекоммуникационных пакетов. Это, при необходимости, позволит властям анализировать трафик и идентифицировать источники преступной деятельности. Данный механизм мог бы стать одним из важнейших средств выявления и идентификации кибернетических преступников.

Однако это, безусловно, вызовет немалые опасения по поводу неприкосновенности частной жизни. Отслеживание информационных потоков означает, что данные о трафике должны храниться в течение какого-то времени. Это серьезный вопрос, выходящий за рамки настоящей статьи, но рассмотрим один из возможных сценариев. Если кто-то незаконно получит доступ к записям данных о трафике, то он сможет их стереть или извлечь необходимую ему информацию, пользуясь методом интеллектуального анализа данных или другими методами, и незаконным путем получить некую выгоду (например, конкурентное преимущество). Данная проблема требует правового регулирования, ограничения доступа и соответствующих решений в области аппаратного и программного обеспечения.

Просвещение требует масштабных и продолжительных усилий, но только так можно добиться наилучших и долгосрочных результатов. Обладая соответствующими знаниями и умениями, пользователь с гораздо меньшей долей вероятности станет жертвой кибернетических преступников. С другой стороны, преступники давно пользуются методами социальной инженерии, чтобы уговорить пользователя «нажать сюда», после чего тот становится их жертвой. Просвещение в этой области необходимо точно так же, как и обучение грамоте несколько веков назад. Однако нужно не только просвещать рядовых пользователей персональных компьютеров, но и повышать квалификацию профессионалов, в особенности, тех кто имеет дело с кибернетической преступностью, не обладая необходимой технической подготовкой: судей, адвокатов и прокуроров ЕС.

В отсутствие более масштабной и общепринятой стратегии борьбы с кибернетической преступностью инициативу взяли на себя частные лица, неправительственные организации, образовательные учреждения и производители систем безопасности, несмотря на различия интересов. Частные лица, некоммерческие организации и ученые уделяют основное внимание необходимости систематического решения проблемы (распространение информации, просвещение, выработка новой стратегии безопасности, открытые программные средства и т.д.), в то время, как производители отчасти стремятся к повышению собственной прибыли.

Координирование шагов по борьбе с преступностью на международном уровне — непростая задача. Подобные шаги требуют участия множества структур, а некоторые из них приступили к их осуществлению, не желая ждать, пока правительства осознают необходимость международного согласия по данному вопросу.

Первый шаг по длинному пути

Нынешнее положение на фронте борьбы с кибернетической преступностью внушает тревогу. Оно напоминает огромную плотину, выстроенную на скорую руку для того, чтобы избежать худшего, но готовую рухнуть в любой момент, вызвав негативные последствия в области безопасности, политики, финансов и социальной жизни. Имеющиеся на настоящий момент механизмы безопасности уже нельзя считать эффективными. Они даже порождают нежелательный побочный эффект — иллюзию безопасности.

При таком положении вещей, когда каждый решает собственные проблемы, все борются с кибернетической преступностью всеми доступными способами. У государства есть законы и механизмы принуждения. У институтов есть защитные механизмы аппаратного и программного обеспечения, созданного и обслуживаемого профессионалами. У частных лиц есть личные системы защиты. Рынок систем компьютерной безопасности растет, стараясь не отставать от злоумышленников. Крупные игроки на рынке систем безопасности получают большие прибыли, но, несмотря на выгоды существующего положения, признают, что их задача становится все более трудной.

Кибернетическая преступность представляет серьезную угрозу для всех, и к ней нужно относиться со всей серьезностью. Простые действия, предпринимаемые только в одной стране, дадут скромные результаты. Имеющееся у нас подобие безопасности может быть в любой момент разрушено кибернетическим преступлением чудовищного масштаба.

На пути к созданию системы активной защиты необходимо преодолеть множество препятствий, одним из которых является отсутствие норм международного права, касающихся преступлений этого типа. Другие проблемы имеют организационный и технический характер, и решить их будет легче в случае создания международно-правовой основы борьбы с этой новой глобальной угрозой. □

НОВАЯ ЭРА ответственности

ИЛЛЮСТРАЦИЯ PER CONCORDIAM

Международная правовая реформа может ввести ответственность государства за кибернетические преступления

Д-р Брет Майкл и Профессор Томас Вингфилд

Низкое качество услуг безопасности, предоставляемых поставщиками информационно-коммуникационных технологий (ИКТ), осложняет и даже делает невозможной реализацию национальных и международных инициатив по противодействию и правовому реагированию на преступную деятельность, террористические акты и военную агрессию в кибернетическом пространстве. В результате кибернетическое пространство стало параллельной вселенной, в которой преступники, террористы и незаконно действующие боевики могут действовать с высокой степенью безнаказанности. Сложность заключается еще и в том, что предоставляемые услуги защиты частной жизни, обеспечивающие анонимность пользователей и шифрование данных, усложняют работу правоохранительных органов, спецслужб и вооруженных сил по отнесению действий (как законных, так и нет) к деятельности отдельных лиц или государств.

Примером может служить широко известный компьютерный червь Стакснет — интегрированный набор вредоносных инструментов, предназначенный для поражения промышленных систем управления определенного образца. Воспользовавшись существенными недоработками в спецификации, реализации и контроле политики безопасности, создатели Стакснет смогли удаленно и анонимно управлять вредоносной программой, выполнявшей все их указания. Зацепок, указывающих на тех, кто разработал или использовал Стакснет, слишком мало. Существует опасение, что Стакснет будет взят за образец при создании вредоносных программ сходного назначения, полагающихся на еще не раскрытые уязвимости в существующих и будущих ИКТ, точно так же, как современные вирусы и черви являются разновидностями описанных в диссертации Коэна или реализованного Моррисом.

Однако проблема ответственности носит не только технологический характер. В международном законодательстве имеются «серые зоны», например, в определении ответственности государства в случае, если негосударственные субъекты предпринимают действия по указанию, при подстрекательстве или под контролем государственных органов. В настоящее время распространены противоречивые правовые оценки неподсудности государства в таких ситуациях. Согласно одной из крайних точек зрения, представленной решением по процессу «Никарагуа против Соединенных Штатов Америки», государство ограждено от ответственности. Другое, более взвешенное мнение было выражено в процессе «Обвинение против Душко Тадича». К чему это нас приводит? В условиях правовой неопределенности в данной сфере, а также легкости проведения тайных нелегальных операций в кибернетическом пространстве, государства заинтересованы в привлечении третьих лиц для осуществления деятельности по их указанию, например, по провоцированию массовых беспорядков и разрушению объектов жизнеобеспечения в интересующем государстве. Недостаток правовой ясности в этом вопросе имеет два следствия: он обеспечивает прикрытие агрессорам, балансирующим на грани закона, а также порождает неопределенность для законопослушной обороняющейся стороны, которая в этих условиях предпочтет воздержаться от действий, способных защитить ее от беззакония.

При существующих технических инструментах - или отсутствии таковых - и в рамках имеющейся правовой системы мы можем ожидать большего числа атак, источник которых трудно или вовсе невозможно отследить с помощью технических средств.

Чтобы считаться международным противоправным деянием, некое действие или бездействие государства должно представлять собой нарушение международных обязательств. Более того, государство расценивается как единый субъект, таким образом, любые государственные действия на любом уровне относятся к государству в целом. Международное право распространяет данные критерии на действия любой группы, чья деятельность может привести к созданию нового государства.

На международном семинаре «Научные и правовые проблемы: создание международных информационных систем безопасности» мы предложили международному сообществу рассмотреть возможность принятия ряда конкретных первоначальных мер, которые бы усложни-

АГЕНТСТВО ФРАНС-ПРЕСС

Ген. Кит Александер, командующий Кибернетическим командованием США и директор Агентства национальной безопасности США, выступает перед комитетом Конгресса, обсуждающим «Подготовку Кибернетического командования США к операциям в кибернетическом пространстве» (сентябрь 2010 г.)

Аналитики в Центре национальной кибернетической безопасности и интеграции средств связи США в штате Виржиния готовятся к учениям по кибернетической безопасности.

АГЕНТСТВО ФРАНС-ПРЕСС

ли деятельность правонарушителей в кибернетическом пространстве, использующих «серые зоны» международного права в своих интересах.

Шаг 1: развенчание мифов

Мы должны развенчать три расхожих заблуждения.

Необходимо соблюдение одного из трех критериев бремени доказывания: отсутствия обоснованного сомнения, ясности и убедительности, а также принципа наличия более веских доказательств. Данные критерии доказанности не относятся к военным и разведывательным операциям. Кроме того, ответственные за решения лица лишь в редких счастливых случаях имеют возможность отследить источник, прежде чем предпринимать действия по предотвращению атаки или реагированию на нее, особенно в кибернетическом пространстве, где имеют место иные масштабы пространства и времени: атаки могут протекать в считанные миллисекунды, а физические расстояния между источником атаки и ее целью в большинстве случаев непринципиальны.

Существует ряд нетехнических методов определения источника возможной атаки. Своевременное выявление источника деяния для организации эффективных мер реагирования зачастую невозможно по таким причинам, как подделка идентификационной информации или отсутствие двусторонних и многосторонних соглашений об обмене данными о маршрутах движения сообщений при пересечении одной или нескольких государственных границ. Учитывая то, как функционируют интернет-протоколы передачи сообщений, это скорее норма, чем исключение. Однако такие факторы не являются непреодолимым препятствием для определения виновности. Для этого существует множество других методик, в частности, данные разведки открытых источников, агентурной и радиоразведки. Отсутствие возможности достоверного отслеживания не исключает использования любых иных источников и методов для получения четкой картины ответственности, возможно, постфактум.

Для действий на международном уровне необходимо определить, что источником деяния является конкретное государство. Напротив, лица и группы лиц могут подвергаться следственным действиям и судебному преследованию в соответствии с внутренним законодательством другой страны, если соблюдено одно из пяти условий, обычно называемых принципами международной юрисдикции:

- территориальный, т.е. действие на территории либо «существенные последствия» на территории
- национальный (активный), т.е. правонарушитель является гражданином данной страны
- национальный (пассивный), т.е. потерпевший является гражданином данной страны
- охранительный, т.е. действие представляет угрозу безопасности для данной страны
- принцип всеобщности, когда преступление степень тяжести преступления столь велика, что любое государство может принять дело к рассмотрению под своей юрисдикцией (например, морское пиратство, рабство, геноцид).

Шаг 2: разработка системы

Нами была предложена разработка правовой системы с целью оценки операций разведывательных и военных структур, осуществляемых в физическом и кибернетическом пространстве, с целью уменьшить правовую неопределенность, связанную с подобной деятельностью. В качестве отправной точки в обсуждении и разработке такой системы мы предложили построение двумерного графика (представленного на схеме ниже), связывающего разведывательную или военную активность с уровнем ответственности государства на основе двух факторов: (i) на степени вовлеченности государства в данную деятельность и (ii) на степени нашей уверенности в вовлеченности государства, оцениваемой, например, по тому, выбирает ли государство объекты нападения, финансирует ли данную деятельность и т.д.

Шаг 3: создание руководства в применении базовых норм права

В целях дальнейшего развития дискуссии и выработки концепции разведывательных и военных операций в кибернетическом пространстве мы рекомендуем, чтобы в процессе составления черновых вариантов базовых норм

права в Комиссии по международному праву были показаны реалистичные примеры подобной деятельности. Такие примеры представляют особую ценность при разработке общего понятийного аппарата и рассмотрении проблем и решений экспертами права, политики и технологий, привлеченными к обсуждению вопросов отслеживания и ответственности. Прошедшая недавно в Москве конференция со всей очевидностью продемонстрировала различия в интерпретации даже общеупотребительных терминов среди участников из разных стран.

Сложности технического характера

В ходе международных дискуссий их участникам стоит иметь в виду, что установление источника несимметрично. Стороны, учавствующие в обсуждении, могут преследовать различные цели и иметь отличные требования к установлению источника: от полного установления до полного неустановления. Установление источника подразумевает соглашение между отправителем, получателем, а также всеми иными сторонами, вовлеченными в обсуждение и сотрудничество в этой связи. Кроме того, нужна уверенность в том, что источник определен верно и точно. Как было отмечено выше, это скорее относительная мера, нежели абсолютная.

Более того, установление источника так и останется нетривиальной с технической точки зрения задачей – панацеи или простых решений не существует. К примеру, при зарождении Интернета необходимость идентификации пользователя не принималась в расчет, а возможность перепроектировать нынешний Интернет с учетом этого требования оказалась нереальной: это бы потребовало существенных изменений в структуре Сети (если не рассматривать всерьез возможность создать все с нуля).

Мы наблюдаем повторение похожих ошибок и в наших инфраструктурах сотовой связи. Многие современные системы, например, глобальная система сотовой связи GSM, полагаются на одностороннюю аутентификацию пользователя и оператора связи, при которой происходит отождествление пользователя перед базовой станцией, но не наоборот, оставляя, таким образом, GSM-сети уязвимыми для действий злоумышленников. На известной конференции о деятельности хакеров DEFCON 18, проходившей в августе 2010 года, один из докладчиков продемонстрировал возможность отключения шифрования сотовой связи в зале, отправив в эфир простую последовательность GSM-команд с помощью ноутбука и антенны.

У пользователей ИКТ есть два варианта: (1) положиться на то, что инфраструктура корректно передаст содержание сообщений, или (2) заранее договориться о том, как контролировать целостность сообщений, не полагаясь на знание маршрута, который сообщение пройдет от отправителя к получателю. В первом случае нет почти никаких гарантий целостности сообщений, прибывающих к получателю, что делает установление источника затруднительным. Во втором случае, как показал Симмонс, возникают технические проблемы, главная из которых заключается в спецификации и корректной реализации методов и протоколов создания, поддержания или даже предотвращения строгой привязки отправителя к передаваемым им сообщениям.

Круг заинтересованных в итогах дискуссии об ответственности государства не ограничен лишь сторонами передачи сообщений и может также включать:

- государства и организации, непосредственно связанные с отправителем или получателем
- государства и организации, не связанные с отправителем или получателем, но заинтересованные в некоторых аспектах положений, переговоров или правоприменения в сфере установления источника

Государства, с территории которых сообщения передаются или по территории которых следуют к месту назначения

- провайдеры услуг связи, таких как доступ в интернет, и операторы сетевых инфраструктур

Выводы

Как лаконично выразились Томас Бюргенталь и Шон Мерфи: «…даже крупнейшие державы имеют долгосрочную и краткосрочную политическую и экономическую заинтересованность в таком международном порядке, при котором конфликты разрешаются в соответствии с общепризнанными правилами и достаточно предсказуемым образом, снижающим вероятность применения силы».

Что действительно требуется, так это решения, которые были бы всеобъемлющими в том смысле, что принимали бы в расчет политические, правовые и технические аспекты, оставаясь в то же время реализуемыми на практике и приемлемыми для государств, не доверяющих друг другу. Учитывая, что вся история международных отношений развивалась с участием тех же сил, трудности интеграции «кибернетического » законодательства, политики и технологий являются не столь непреодолимыми. □

Взгляды и суждения, изложенные в настоящей статье, являются личными взглядами авторов и не должны рассматриваться как отражающие (прямо или косвенно) официальную политику Правительства США.

1. Дополнительные сведения о Stuxnet можно найти, например, здесь: http://en.wikipedia.org/wiki/Stuxnet.
2. Ф. Коэн, «Компьютерные вирусы», докторская диссертация, Университет Южной Калифорнии, 1986.
3. Дж. Маркофф, «Компьютерному злоумышленнику назначили пробацию и штраф в $10,000,», газета «Нью-Йорк Таймс» от 5 мая 1990 г., стр. 9.
4. «Военные и полувоенные действия в Никарагуа и против него (Никарагуа против США)», 1986 г. Международный Суд ООН 14, 100-1 (от 27 июня).
5. «Обвинение против Душко Тадича (Решение суда об обжаловании обвинительного приговора)», IT-94-1-A и IT-94-1-Abis, Международный трибунал по бывшей Югославии (ICTY), 26 января 2000 г..
6. Семинар проводился в ноябре 2010 года в Московском Государственном университете им. Ломоносова в рамках 6-й Международной научной конференции по проблемам безопасности и борьбы с терроризмом.
7. Проекты статей «Об ответственности государств за международную незаконную деятельность» с комментариями – ООН, ежегодное издание Международной правовой комиссии, 2001, Том II, Часть 2.
8. См. http://www.computerworld.com/s/article/9179959/Hacker_snoops_on_GSM_cell_phones_in_demo
9. Г. Дж. Симмонс, «Каналы подсознания: прошедшее и настоящее», опубл. в «IEEE Европейские операции в сфере телекоммуникаций», Том 5, стрр. 459-473, 1994 г.
10. Томас Бергенталь и Шон Д. Мерфи, «Международное публичное право вкратце», Св. Пол (Миннесота, США): West Group, 4е издание, 2006 г..

РЕЙТЕР

Для стимулирования ветровой и солнечной энергии в Европе крайне необходимо сотрудничество

«Электризующее» начало

Удачная комбинация энергетического спроса и предложения — растущий парк электрических и гибридных автомобилей, двигающихся за счет энергии ветряных мельниц в Северном море и солнечных панелей вдоль средиземноморского бассейна, – в ближайшее десятилетие полностью изменит европейскую транспортную систему.

Двигателем преобразований служат недавно подписанные международные соглашения об улавливании, хранении и передаче генерирующих энергию морских ветров, совместно с положениями, вступающими в силу в 2014 году, согласно которым в 27 государствах Евросоюза должны использоваться двигатели более полного сгорания.

Совместно разработанный подход ЕС направлен на решение целого ряда наболевших проблем континента: загрязнение воздуха ввиду чрезмерного использования электричества, генерируемого за счет сжигания угля, ненадежность поставок нефти и газа и не внушающий оптимизма экономический рост, подрывающий способность Европы к самообороне и защите своих ценностей.

«Чтобы поставить нашу энергосистему на новый, более устойчивый и безопасный, путь, потребуется время, но смелые решения в этом направлении надо принимать уже сейчас, - заявил в ноябре 2010 года комиссар по вопросам энергетики ЕС Гюнтер Эттингер. – Для того чтобы иметь эффективную, конкурентоспособную и мало зависящую от углеродов экономику, мы должны европеизировать нашу энергетическую политику и сосредоточиться на новых, но крайне актуальных приоритетах».

Немалую часть в этой политике занимает внедрение положений «Евро 6», нацеленных на снижение выхлопов выводящих труб транспортных средств, начиная с 2014 года. «Евро 6», в целом, рассматривается как способ подтолкнуть автопроизводителей к созданию электромобилей и сокращению производства автомобилей на дизельном топливе, составляющих практически половину всех продаж автомобилей в Европе. Дизельная автопромышленность не исчезнет, однако, требования к сокращениям выхлопов вынуждают крупных производителей, таких как «Мерседес», «Вольво», «Пежо» и «Фольксваген», разработать дизельно-электрические гибриды, чтобы удовлетворить требования регулятора. В 2010 году министры ЕС пришли к соглашению о том, что, хотя двигатели, работающие на бензине и дизельном топливе, «останутся в отрасли на кратко- и среднесрочный период», электромобили являются «многообещающей, потребляющей исключительно низкое количество углеродов» технологией, которая снизит зависимость ЕС от импортного ископаемого топлива.

«Одним из значительных положений «Евро 6» являются достаточно суровые требования к дизелю», - заявил

новостному агентству «Bloomberg» аналитик лондонской «IHS Automotive» Колин Каучман в конце 2010 года. Согласно новым правилам, двигатели должны выбрасывать на 56% меньше оксида азота – сокращение, которое по силам немногим дизельным двигателям в 2010 году. Автопроизводители заявляют, что экологическое законодательство приведет к росту производственных издержек, однако, пока неясно, в какой мере эти издержки лягут на плечи потребителей.

Европейцы работают над стандартизацией розеток и зарядных станций, пытаясь решить, применять ли европейские, азиатские или американские стандарты зарядки. Скорость перезарядки крайне важна, поскольку большинство электромобилей могут проехать всего примерно 100 км до того, как их необходимо снова подключить к электросети. Чтобы продажи электромобилей стали популярными, покупатели не должны ждать по 8 часов, пока машина перезарядится. «Золотым стандартом» является получасовая зарядка. В 2009-2010 гг. Венгрия, Нидерланды, Германия, Португалия, Хорватия и другие страны создали прототипы, как они надеются, будущих национальных станций зарядки автомобилей.

В октябре 2010 года португальский министр энергетики Карлос Зорриньо объявил о том, что, начиная с 2011 года, система станций зарядки вырастет до 1300 станций, расположенных в 25 городах страны. «Станет возможным проехать через всю страну, без проблем перезаряжая электромобиль», - заявил Зорриньо агентству «Рейтер». По имеющимся сведениям, Венгрия открыла первую общественную станцию зарядки электромобилей в Секешфехерваре в сентябре 2010 г. В мае 2010 года Нидерланды открыли одну из первых на континенте станцию быстрой перезарядки в городе Леуварден.

В 2009 году, на автоярмарке во Франкфурте, «Рено» предложила еще один способ преодолеть ограниченный набор автомобилей, работающих исключительно на электричестве. Континентальная программа обмена, основанная на старинном принципе перекладных карет, которым требовалась смена лошадей после пробега определенного интервала, позволит автовладельцам заменить арендованную батарею, у которой зарядка подходит к концу, на полностью заряженную.

Сами по себе электромобили не являются панацеей. Европа уже эффективно производит «чистые» дизельные автомобили, которые вписываются в стандарты топливной экономики без грязных выбросов, ассоциирующихся с предыдущими поколениями двигателей, работающих за счет сжигания мазута. «Пежо», второй по величине производитель автомобилей в Европе, ожидает, что, начиная с 2015 года, продажи гибридных автомобилей ежегодно составят 100 тыс. машин. Эта цифра равна менее 5% ежегодного сбыта «Пежо», продающей свыше 3 млн. легковых автомобилей и грузовиков в год.

Цена электромобиля, по крайней мере, сначала, может перевести его в категорию «люкс», хотя он и не обладает «люксовскими» характеристиками. Ценники на электромобилях почти в два раза выше, чем на подобных им по набору характеристик экономичных автомобилях. Как заявил в статье журнала «Der Spiegel» от декабря 2010 года один из руководителей немецкого автопрома Райнер Курек, электромобили будут пользоваться успехом как дешевый вид транспорта, но не

РЕЙТЕР

Вращающиеся ветряные мельницы в Horns Rev 2 – одной из крупнейших в мире ветровых электростанций, расположенной у западного побережья Дании. Проект был запущен в 2009 году и будет способствовать снижению зависимости Европы от тепловой энергии угля.

Водитель включает свой электромобиль в электросеть на зарядной станции в Дрездене в августе 2010 г. Немецкая земля Саксония установила станции перезарядки батарей, часть из которых может быть включена в будущую континентальную зарядную сеть.

как статусный автомобиль для богачей. «Такие машины могут удовлетворить лишь очень ограниченную потребность в перемещении и не годятся в качестве дорогих и престижных», - сказал Курек.

«IHS Automotive» сообщила «Bloomberg», что ожидает повышения продаж электрических и гибридных автомобилей, вызванного положениями «Евро 6», до около 13 процентов в 2020 году, по сравнению с 0,1% в 2010 году. «Automotive News Europe» дает менее оптимистический прогноз агентству «J.D. Power and Associates», согласно которому электромобили и гибриды достигнут лишь 7% продаж в Европе в ближайшее десятилетие. Председатель «Фольксвагена» оказался менее увлечен тем, что он сам назвал «электролихорадкой». В обращении 2009 года, приведенном немецкой газетой «Handelsblatt», его прогноз продаж электромобилей в 2020 году составляет менее двух процентов в мире, а неминуемая гибель двигателей, работающих на бензине, по его словам, существенно преувеличена.

Что же касается снижения уровня загрязнения, то электромобили экологичны настолько, насколько экологично подаваемое в них электричество. Например, в Польше, где бо́льшую часть энергии получают за счет сгорания угля, электромобили не приведут к снижению загрязнения атмосферы, как, например, во Франции, где электричество добывается, в основном, за счет безвыбросовой ядерной энергии. Здесь на сцену выступают ветровая и солнечная энергия. В амбициозные планы ЕС входит добиться 20% обеспечения государств-членов возобновляемой энергией к 2020 году и 50% – к 2050 г.

На ветер лучше всего рассчитывать в Северной Европе, где генерация солнечной энергии недостаточна из-за частой облачности региона. В декабре 2010 года 10 стран объявили о соглашении создать энергетическую «суперсеть» на Северном море для сбора и распределения ветряной энергии. Это - Германия, Франция, Великобритания, Швеция, Дания, Ирландия, Голландия, Люксембург, Норвегия и Бельгия. Признавая ветровой потенциал региона, сторонники соглашения видят Северное море «Саудовской Аравией возобновляемой энергии». «Крупномасштабные объединения энергосистем между европейскими соседями крайне важны, если мы собираемся объединить колоссальный потенциал морских ветров и интегрировать его на европейские рынки», - заявил в декабре 2010 года Гордон Эдж, руководитель торговой ассоциации по возобновляемой энергии Великобритании «RenewableUK».

Более сложные схемы ведут дальше за границу. Тридцать европейских компаний образовали консорциум «Desertec Industrial Initiative», который пытается «раскрутить» инвесторов на проект разработки североафриканских солнечных и ветровых станций, стоимость которого составляет 400 млрд. евро. В случае удачи, к 2013 году «Desertec» сможет построить свою первую электростанцию. Сторонники проекта считают, что он станет одним из крупнейших инфраструктурных программ в истории, если ему удастся добиться своей цели поставлять 15% энергии для Европы к 2050 году. «Desertec» намеревается улавливать солнечную энергию двумя способами: с помощью отражающих зеркал, направленных на солнечные лучи, для нагрева турбин, и с помощью фотогальванических элементов, напрямую захватывающих солнечную энергию.

Проект включает в себя целую массу проблем, не последнюю роль из которых играет стоимость северо-африканской энергии, которая стоит вчетверо больше энергии, добываемой за счет сжигания угля и газовых генераторов. «Desertec» пытается добиться от ЕС льготных условий, особенно, в форме субсидий. К тому же, оказывается, непросто получить поддержку к югу от Средиземноморья. Хотя потенциальные партнеры, такие как Марокко и Египет, положительно оценили проект, Алжир более склонен к строительству собственных солнечных станций («Bloomberg Businessweek», сентябрь 2010 г.). «Европейские страны могут развиваться в этом направлении быстрее и дешевле, чем если «Desertec» будет поставлять возобновляемую энергию из природных источников», - заявил «Businessweek» Герман Шеер, член немецкого парламента и глава компании «Eurosolar», исследовательской группы, изучающей солнечную энергию. Многообещающе выглядит и испанская солнечная энергия, хотя в докладе ЕС 2010 года говорится о том, что передача избыточного испанского электричества во Францию потребует утроения мощности линий электропередач.

Однако если большинство проектов удастся, «зеленые» машины и производители возобновляемой энергии смогут создать сотни тысяч новых рабочих мест, чтобы частично сбалансировать потерянные рабочие места в отраслях, зависящих от традиционной генерации электричества. Технологии, разработанные в Германии и Франции, включая зарядные станции для автомобилей и инновации в области лопастей ветряных мельниц, могут экспортироваться соседям ЕС в Восточной Европе и Центральной Азии. Более того, проект строительства североафриканских солнечных станций потребует высокого уровня международного сотрудничества, что приведет к созданию новых предприятий, выгодных для развивающегося региона, поставляющего Европе бо́льшую часть нелегальных иммигрантов.

Энергетическая независимость будет расти. Природный газ, используемый для нагрева европейских электротурбин, помимо прочих стран, поступает из России и Алжира. Горючее для производства бензина и дизельного топлива является главным экспортируемым продуктом из стран Ближнего Востока и России. Экологически чистые внутренние поставки топлива могут частично разорвать узы, связывающие ЕС с не всегда дружественными режимами. Согласно докладу Европейской ассоциации ветровой энергии 2010 года, ветровые мощности росли в 2009 году быстрее, чем любой другой энергоисточник. Независимо от того, является ли выделяемый в результате деятельности человека углекислый газ основным фактором того, что считается глобальным потеплением, сокращение вредных выбросов полезно для общества. □

От враждебности к гостеприимству

Спокойствие на Кавказе может содействовать возрождению туризма в регионе

В октябре 2010 года грузинский президент Михаил Саакашвили, окруженный газетчиками и телерепортерами, снял с себя рубашку и нырнул в Черное море на трехкилометровый заплыв. Целью эффектного выступления Саакашвили являлось экономическое возрождение грузинского побережья вокруг города Батуми, популярного в советское время туристического центра, жаждущего возобновления туризма, приносящего евро и доллары. В промежутках между подобными испытаниями на выносливость Саакашвили также похвалил полуразрушенную горнолыжную отрасль в горной части страны.

«Десятки лет мы объясняем европейцам, что Грузия может быть Швейцарией на Кавказе. Нигде в мире нет такого сочетания морских и горнолыжных курортов – и это без преувеличения, - заявил президент новостному сайту «Georgia Today» в 2010 году. – Так давайте, вместо того, чтобы стать Швейцарией на Кавказе, сделаем Швейцарию европейской Грузией. … Чтобы другие сравнивали себя с нами; а пока Грузии нужно много работать, и ей нужно много инвестиций».

За два десятилетия после падения Советского Союза политическая и экономическая нестабильность разогнали большинство туристов, любителей субтропических пляжей региона, игристого вина, каменистых скал и исторических мест.

Местия – село в грузинском районе Сванетия – надеется привлечь больше лыжников и других путешественников.
АГЕНТСТВО ФРАНС-ПРЕСС

Однако в этот относительно удаленный уголок Евразии, включающий в себя Грузию, Армению, Азербайджан и некоторые части России, грядет туристический ренессанс.

У туристов сейчас намного больший выбор. Армения протянула самую длинную канатную дорогу в мире (5,7 км) над ущельем реки Воротан, которая ведет в знаменитый Татевский монастырь, построенный в 9 веке. В окруженном сушей государстве к северу от Турции экономическое восстановление ведет к наплыву исследующих достопримечательности армян, живущих за границей, - явление, известное под названием «туризм диаспоры». Азербайджан стремится быть «элитарным» туристическим направлением, обладающим прелестями Ирана без политических и религиозных недостатков соседа. В 2010 году газета «Caspian Business News» писала, что Азербайджан потратил четыре предыдущих года на реставрацию и строительство 370 гостиниц вместимостью в 30 706 номеров. Как часть «ребрендинга», предназначенного для иностранных туристов, Грузия начала кампанию по борьбе с загрязнением окружающей среды с целью создания «золотых песочных пляжей» из прибрежной части Батуми к 2012 году.

Самой крупной инвестицией в сферу туризма в регионе является многомиллиардный капремонт черноморского города Сочи – столицы Зимних Олимпийских игр 2014 года, где пальмовые деревья раскачиваются на фоне снежных горных вершин. Чтобы справиться с многочисленной толпой туристов, Москва выделяет средства на самый крупный строительный проект в Европе – «с нуля» строятся лыжные павильоны, хоккейные и конькобежные арены, стадион на 69 тыс. человек, 90 тыс. номеров гостиниц и высокоскоростные железнодорожные линии.

«В настоящее время «Сочи-2014» является одним из крупнейших комплексных инвестиционных проектов в мире. Одновременно ведется строительство более 800 отдельных строительных проектов, которые завершатся к 2014 году. Успешное завершение этих проектов создаст более 50 новых предприятий и 43 тыс. рабочих мест», - заявил российский вице-премьер Дмитрий Козак в мае 2010 года.

Во времена Советского Союза Кавказ, прозванный «русской ривьерой», был экзотической альтернативой ледяного севера. Его горные склоны и морские прибои были в почете у коммунистов-аппаратчиков, развлекавшихся там с женами и подругами. Морские санатории, своей чванливостью напоминающие советские и даже царские времена, сменяются лыжными базами у горных подножий черноморского побережья. Чуть дальше вглубь страны расположено «царство приключенческого туризма» - идеальная местность для иностранцев в поиске покорения труднодоступных горных деревень и одиноких, удаленных от всего мирского, монастырей. Курортную

АССОШИЭЙТЕД ПРЕСС

Строительство подъемника вблизи Сочи – места проведения Зимних Олимпийских Игр 2014 года. Игры должны привлечь тысячи туристов на Кавказ – регион, пытающийся оживить свою экономику.

атмосферу дополняют вина и коньяки, в изобилии производимые в регионе.

Тем не менее, еще одна главная черта Кавказа – десятки проживающих в регионе народностей и десятки языков – привела к вспышкам насилия, особенно после того, как тяжелая рука Советской власти ослабила свою хватку. Среди самых резонансных споров, – так называемые, «замороженные конфликты» в Южной Осетии, Абхазии и Нагорном Карабахе.

Новый посол США в НАТО Курт Волькер призвал международное сообщество к тому, чтобы использовать Олимпийские Игры в Сочи как возможность урегулирования конфликтов в регионе. В статье, опубликованной газетой «The Christian Science» в мае 2010 года, Волькер выражает обеспокоенность тем, что открытое признание Россией независимости Абхазии и Южной Осетии - двух регионов, отделившихся от Грузии при поддержке России, - омрачит игры. Самопровозглашённые абхазские и южноосетинские лидеры объявили независимость от Грузии в начале 1990-х годов, однако, только в 2008 году грузинские власти были вытеснены с помощью российских вооруженных сил. Дипломатическое признание отделившихся республик минимально: страны НАТО, ЕС и Организации по безопасности и сотрудничеству в Европе считают данные территории частью Грузии.

«Олимпийские игры в Сочи могут стать катализатором для разрешения замороженных конфликтов и перевести кавказский регион в XXI век», - заявил Волькер. Интерес России в успешном проведении Олимпиады «должен быть мощным стимулом для Москвы… оставить в прошлом ее… привычный подход к Кавказу. Это, несомненно,

«Олимпийские игры в Сочи могут стать катализатором для разрешения замороженных конфликтов и перевести кавказский регион в XXI век ... »

было бы наилучшим результатом для государств и народов региона, для Москвы, для спортсменов и для Олимпиады».

Пример возможности быстрого возрождения туризма – Аджария, прибрежный район Грузии к северу от турецкой границы. В 2009 году Аджарию посетили около 162 тыс. иностранных туристов – рекорд постсоветского времени, - всего год спустя после того, как грузинские и российские войска с оружием в руках боролись за Южную Осетию и Абхазию. Возможность денежных потоков за счет туризма может решить также и разногласия относительно Нагорного Карабаха - населенной преимущественно армянами части Азербайджана, что привело к кровопролитию между двумя странами в 1991 году. Открытая война была прекращена в 1994 году, однако, страх возобновления военных действий на долгие годы уничтожил туризм на Южном Кавказе.

Процесс выздовровления уже начался. В 2010 году была проведена туристическая ярмарка в Ереване (Армения), на которой побывали профессионалы индустрии путешествий из Турции, США, Чехии и Германии. Правительство Армении заявило, что рост туризма в стране составляет около 25 процентов в год, начиная с 2001 года, когда страна отпраздновала 1700-летие христианства в Армении. Туризм в Азербайджане также переживает возрождение, благодаря своим отелям и курортам, сосредоточенным, в основном, вокруг г. Баку на Каспийском побережье. В статье, опубликованной в «EurasiaNet» в 2010 году, рассказывается о строительстве пяти международных люксовых отелей в городе, включая сети «Four Seasons», «Hilton» и «Kempinski». Больше всего в туризм вовлечены турецкие бизнесмены, пользующиеся родственностью турецкого и азербайджанского языков.

«Это проблема, над которой Россия, США и Европа работают уже много лет, и результаты возможной договоренности уже давно предложены, - писал Волькер в 2010 году. – Урегулирование армяно-азербайджанского конфликта обеспечит прилив туризма, торговли, инвестиций и экономического процветания в регионе».

Некоторая непреклонность, оставшаяся со времен СССР, является препятствием для роста туризма. В докладе по Южному Кавказу Всемирный Банк указал, что правительства государств региона слишком медленно свертывают дорогую, действующую «от верхов в низы» гостиничную систему, созданную по модели «Интуриста» - громоздкого, всепроникающего советского турагентства, по совместительству занимающегося шпионской деятельностью во времена Холодной войны. «Интерпретация роли и обязательств подобных институтов не всегда соответствует потребностям рыночной экономики, - говорится в отчете. – Нужно ли упорствовать в чрезмерном контроле во вред стимулированию инвестиций в частный сектор?» Что же касается российских туристов, Турция принимает у себя миллионы путешественников, ранее отдыхавших на Кавказе. В статье 2007 года о российско-турецком туризме, «Guardian» пишет о том, что россиянам дешевле лететь в Турцию, чем в Сочи. «Даже проживание в дачной гостинице в ближайшем Подмосковье стоит больше, чем отпуск в Турции», - добавляет «Guardian».

Тем не менее, Кавказ, особенно Грузия, делает все возможное, чтобы привлечь больше туристов. Страна предлагает обучение гостиничному управлению, включающее в себя прохождение практики в пятизвездочных гостиницах в Турции. Недавно назначенная на пост министра по туризму Майя Сидамонидзе удивила своим предложением «туристического альянса» с Турцией, Арменией и Азербайджаном с целью организации путевок, включающих в себя посещение нескольких стран. Для привлечения частных игорных заведений и гостиниц Грузия отозвала лицензионные платежи и НДС. Туристические визы уже не нужны жителям более 30 стран.

Главным вдохновителем остается Саакашвили, который, помимо зазывания в морские волны, оказывает поддержку большим инвестициям, в надежде превратить грузинский горный район Сванетию в густонаселенный туристами альпийский курорт к 2011 году. Капитальный ремонт трассы и аэропорта, стоящий приблизительно 25 млн долл. США, обеспечит доступ к столице области - городу Местия. В статье, опубликованной в «EurasiaNet» в октябре 2010 года, глава региональной администрации Шмаги Нагани говорит о том, что лыжники и любители природы являются основой создания рабочих мест в этом удаленном районе близ российской границы. «Туризм, вообще, является единственной возможностью для экономического развити этого региона», - заявил он. □

Защита прав афганских женщин

Успех миссии МССБ прекратит террор со стороны Талибана

В 2001 году Афганистан принял новую конституцию, обеспечивающую равенство полов перед законом. В результате, за последнее десятилетие, политическое и культурное положение женщин в Афганистане значительно улучшилось. Впервые за всю историю страны женщины становятся выпускницами академии национальной полиции, вступают в ряды афганских вооруженных сил и занимают влиятельные должности в правительстве, включая посты губернаторов провинций. Тем не менее, афганские женщины боятся, что улучшения последнего десятилетия окажутся под угрозой, если Международные силы содействия безопасности выйдут из страны до завершения миссии. Они обеспокоены тем, что их новоприобретенные права будут потеряны, если к власти снова придет Талибан.

Более 1 тыс. женщин служат в афганских ВС. Они проходят полугодовую подготовку в женской академии в Кабуле, которая готовит их к занятию должностей в администрации, коммуникациях, тыловом обеспечении и медицинской службе. Женщин обучают обыскивать частные дома и проводить патрулирование и проверки на дорогах наряду с офицерами-мужчинами. Они особенно полезны в этой роли, потому что в афганской культуре мужчинам не положено обыскивать женщину или ее сумки. Тем не менее, привлечение новых кадров - сложная задача, ввиду постоянных угроз Талибана в адрес военнослужащих женщин.

«Мы не можем и не должны ждать, пока эти угрозы, риски и проблемы исчезнут сами по себе. Мы должны бороться с ними и преодолевать их, строить лучшую жизнь в стране, - заявила по «Радио Свободная Европа/Радио Свобода» генерал Хатул Мухаммадзай, высокопоставленный офицер-женщина афганских ВС. – В войсках международной коалиции много женщин-иностранок, защищающих наш народ. Для нас же Афганистан - это родной дом. Почему же мы не должны служить родной стране?»

Корпус морской пехоты США сумел наладить отношения с афганскими женщинами посредством «женских команд взаимодействия». После прохождения ускоренного курса обучения всему, «что можно и чего нельзя» в местных традициях обращения с женщинами, Морские Пехотинцы повязывают под шлемами головные платки и отправляются завоевывать доверие сельских жительниц Афганистана, приходя в их дома, оценивая их потребности и собирая информацию. В афганской культуре женщинам не принято разговаривать с мужчинами-военными, таким образом, общение с женскими делегациями дает афганским женщинам редкий шанс говорить откровенно. Согласно протоколу команды, сначала необходимо получить разрешение у старейшины-мужчины обратиться к деревенским женщинам, распространить лекарства, чай и принадлежности для школы, а затем поговорить по душам. Цель – завоевать доверие этих женщин. «Для нас это хорошая новость. Женщины-морские пехотинцы приехали и поговорили с женщинами, узнали их проблемы. Я очень этому рад», - поделился с Корпусом морской пехоты в статье, опубликованной на сайте МССБ в декабре 2009 года, афганский сержант.

Войска МССБ также предлагают медицинскую помощь афганским женщинам и

АГЕНТСТВО ФРАНС-ПРЕСС

Женщины-офицеры Афганской национальной армии на церемонии окончания академии в Кабуле в сентябре 2010 г.
В настоящее время Армия насчитывает 100 тыс. военнослужащих и планирует вырасти до 240 тыс..

детям. Часто матери и дочери не обращаются за медицинской помощью из страха, что их будет осматривать доктор-мужчина. Некоторым требуется преодолеть долгий путь и пересечь границу страны, чтобы получить приемлемую медицинскую помощь в Пакистане. Для многих медицинская помощь со стороны военнослужащих МССБ – первая в их жизни.

Вовлечение женщин важно для усиления безопасности. Женщины-новобранцы могут пополнить ряды афганских сил безопасности на 80 - 160 тыс. это то количество, необходимое, по подсчетам афганского МВД, для борьбы с повстанцами. Еще 16 женщин окончили полицейскую академию в Кабуле в августе 2010 года, пополнив ряды сотен женщин на службе. Женщины-полицейские обеспечивают в Афганистане важную функцию.
Согласно данным «Радио Свободная Европа/Радио Свобода», они лучше осведомлены, как обращаться с преступницами и могут обыскивать женщин; само их присутствие помогает преодолеть отрицательные стереотипы. Тем не менее, женщины-полицейские «часто становятся жертвами плохого обращения или выражения общественного презрения тех, кто считает, что они должны жить в соответствии с более традиционным укладом жизни», - говорится в докладе. Стажеров академии обучают проводить обыски домов, обезвреживать взрывные устройства, обращаться с огнестрельным оружием, проводить аресты и выявлять контрабанду наркотиков.

Афганские женщины также расширяют свое присутствие в правительстве страны. Парламентские выборы сентября 2010 года показали, сколь много добились женщины. Согласно данным «Deutsche Welle» от ноября 2010 года, шестьдесят девять кандидаток получили места в Волеси Джирга – нижней палате Национальной Ассамблеи Афганистана - из 249 имеющихся в палате. Конституция Афганистана установила 25%- ную квоту количества женщин в Волеси Джирга, однако, женщины превзошли эту квоту, получив 28% всех мандатов. Женщины начинают также занимать все больше кабинетных должностей. Согласно данным «Reuters», в январе 2010 года президент Хамид Карзай предложил назначить трех женщин на должности в новом кабинете.. Защитникам прав женщин и Карзаю был нанесен серьезный удар, когда утвердили только одну. «Возможно, еще слишком рано ожидать многого от парламента, находящегося под влиянием консервативных элементов», - прокомментировала ситуацию активистка борьбы за права женщин Орзала Ашраф Немат лондонской газете «The Telegraph» в январе 2010 года.

Женщины стремятся улучшить свое положение даже в традиционно управляемых частях страны. Подпольные школы и секретные убежища – вот некоторые из единственных возможностей самозащиты и самосовершенствования этих женщин. В апреле 2010 года британская газета «The Independent» писала о том, что тайные занятия грамотой проводятся под прикрытием встреч для совместной молитвы в десятках деревень провинции Забул. «Уроки ориентированы на обучение грамоте пушту, арифметике, вопросам здоровья и гигиены», - объяснил в апреле 2010 года «The Independent» Есанулла Есан - человек, стоящий за созданием подпольных школ. В статье рассказывается о том, как он проводит обучение на школьной доске, если ему не удается тайно провезти учебники, и надеется расширить программу образования, включив в нее историю, науку и этику. Дети также, как никогда ранее, посещают школу. Количество афганских детей, обучающихся в начальной школе, превысило все предыдущие рекорды и составило 6 миллионов человек. Образование – это единственная возможность для женщин разорвать замкнутый круг подавления их прав – круг, работающий в пользу таких групп, как Талибан.

Несмотря на достигнутый прогресс, в сельских областях продолжается подавление прав женщин. Оскорбительное отношение мужа, насильственное вступление в брак, строгие ограничения в перемещении в обществе и отказ в образовании по-прежнему стоят на пути женщин. В отношении некоторых женщин Талибаном все еще применяются пытки.

Афганские полицейские-женщины приветствуют женщину-представителя Службы США по связям с гражданской администрацией и населением во время церемонии, посвященной Международному женскому дню, в марте 2010 года в Лашкар-Га. Женщины США и Афганистана сотрудничают и обсуждают успехи и трудности деятельности, связанной с женским вопросом.

АГЕНТСТВО ФРАНС-ПРЕСС

Согласно докладу «U.N. Dispatch» от ноября 2010 года, иногда афганские женщины поджигают себя, чтобы, устав от принуждения и насилия, покончить с собой.

Подобные же сведения появились и в статье 2010 года журнала «Time», рассказывающей о жизни женщин при Талибане. Аиша, восемнадцатилетняя девушка, фотография которой размещена на обложке, была наказана полевым командиром Талибана за то, что сбежала из дома своего мужа, потому что, по ее словам, с ней жестоко обращались его родители. С позволения Талибана, деверь девушки держал ее, пока ее муж отрезал ей уши и нос. Ее оставили умирать, захлебываясь в крови и теряя сознание от боли. Аиша была спасена войсками МССБ, и ей была оказана медицинская помощь. Сегодня она – одна из тех женщин, которые боятся возвращения Талибана.

Правила, введенные Талибаном, по-прежнему, исполняются в некоторых сельских территориях. Они включают в себя запрет для женщины на любую деятельность вне стен дома, если только она не сопровождается «махрамом» - близким родственником - мужчиной, т.е. отцом, братом или мужем. Женщинам запрещено ездить на велосипеде или участвовать в спортивных мероприятиях, и их жестоко избивают, если оголится хотя бы лодыжка. Талибан требует закрашивать окна в домах, чтобы женщин нельзя было увидеть через окно с улицы. Свою волю талибы навязывают с помощью доставляемых по ночам писем. «Предупреждаем тебя - либо ты прекратишь учительствовать, либо отрежем головы твоим детям и подожжем твою дочь», - говорится в одном из писем, приведенных в статье «Time».

Афганские женщины в более прогрессивных частях страны добились многого за последнее десятилетие и не желают возвращаться к варварским традициям. Они признают, что им многого еще предстоит достичь. Согласно «Deutsche Welle» от октября 2010 года, хотя они и занимают правительственные должности наравне с мужчинами, как это требуется по закону, многих из них не воспринимают всерьез. «К ним не прислушиваются, и у них нет шансов как-либо повлиять на ход переговоров», - заявила защитник прав женщин Сорайя Парлика. Она также сказала, что некоторые женщины добиваются важных правительственных должностей с помощью связей и взяток, а не благодаря своим способностям.

Руководители стран мира выразили поддержку защите прав афганских женщин. В статье «Reuters» от июля 2010 года говорится о «личном обещании» Госсекретаря США Хиллари Клинтон добиться гарантии прав женщин в будущей политической системе Афганистана. НАТО тоже берет на себя это обязательство: «НАТО поддержит политическую договоренность между правительством Афганистана и Талибаном только в случае соблюдения конституционных прав женщин», - заявил в октябре 2010 года генеральный секретарь НАТО Андерс Фог Расмуссен. Он также добавил, что «в отношении прав женщин был достигнут прогресс – больше девочек посещают школу, больше женщин работают в парламенте и больше женщин, открывающих и управляющих предприятиями или вступающих в ряды полиции. Все это доказывает – и достаточно конкретно - что достигнут прогресс в вопросе прав афганских женщин».

TIME

Августовский выпуск журнала «Тайм» рассказывает об Аише, 18-летней девушке из Афганистана, изуродованной по приказу Талибана за побег из дома своего мужа.

Британская газета «the Guardian» считает, что наилучший путь для защиты прав афганских женщин – это развитие самого Афганистана. В сентябрьском выпуске 2010 года говорится: «Это также потребует активных действий на местном уровне, чтобы афганцы могли получать необходимые услуги, и отлаженного партнерства с неправительственными организациями, потому что на данный момент только они способны полномасштабно действовать на местном уровне».

Может потребоваться много лет, прежде чем афганские женщины добьются равенства с мужчинами, ведь страна только выиграет, воспользовавшись скрытыми талантами половины своего населения. □

О пользе реформ в Центральной Азии

Страх перед региональной нестабильностью побуждает к сотрудничеству

Самарканд, Бухара, Мерв, Ташкент и Ош – древние города Шелкового пути, история которых насчитывает тысячи лет. Жители этих городов пережили взлеты и падения многих империй за свою историю и теперь оказались в государствах, вышедшими из бывшего Советского Союза: Узбекистан, Таджикистан, Кыргызстан, Туркменистан и Казахстан. С момента распада СССР в 1991 году каждое из этих государств создавало свою национальную идентичность как часть более крупного международного сообщества. Ныне специалисты по Центральной Азии все больше обеспокоены тем, что этот богатый ресурсами и критически важный с геополитической точки зрения регион может стать очагом несостоявшихся государств, которые так и не смогли достаточно развиться с момента своей независимости.

Евросоюз и НАТО выразили интерес в предоставлении помощи государствам Центральной Азии в установлении стабильных, безопасных, свободных и процветающих обществ. Бывший государственный секретарь США Кондолиза Райс сказала в интервью «Вашингтон Пост»: «Через слабые и близкие к упадку государства пролегают всемирные маршруты распространения распространения пандемий, перемещения преступников, террористов и самых опасных видов оружия».

Местные проблемы – международное влияние

Возможность нестабильной и слабеющей Центральной Азии является угрозой для Европы и остального мира. Регион, граничащий на юге с Афганистаном, уже столкнулся с проблемой воинственных исламистских групп, самые известные из которых - «Исламское движение Узбекистана», или ИДУ, и Союз исламского джихада, или СИД. ИДУ и СИД связаны с Аль-Каидой и Талибаном. Совсем недавно, в ноябре 2010 года, таджикские силы безопасности вели операции в долине Рашт против, предположительно, экстремистов из ИДУ после побега нескольких влиятельных боевиков из тюрьмы столицы Душанбе.

Сотрудничество между правительствами региона и поддержка ЕС и соседних держав, таких как Россия и Китай, может помочь стабилизировать регион и содействовать его экономическому росту. Проблема создает почву, на которой Россия и Запад могут сотрудничать после десятилетий Холодной Войны. Однако, при всей значительности цели, путь к ней усеян препятствиями.

РЕЙТЕР

Сотрудники российской энергетической компании «Лукойл» проводят инспекцию труб на газовом месторождении Хаузак, расположенном в 350 км к северо-западу от Бухары (Узбекистан). Это месторождение является частью проекта по производству одной пятой части газодобычи Узбекистана.

Пограничный конфликт

Этнические трения в регионе, подобные тем, что произошли в Кыргызстане, сдерживают сотрудничество между центральноазиатскими правительствами. Историю этих противоречий можно проследить вплоть до создания советских республик Центральной Азии в 1924 году, когда, по высказываниям «The Economist», «Сталин сделал из нее лоскутное одеяло из республик, чьи границы были созданы с целью дробления рас и уничтожения национализма. Он преуспел в том, чтобы помешать этническим группам объединиться против него, и в том, чтобы каждая республика стала очагом этнических распрей».

Природные ресурсы являются основным источ-

ником трений между правительствами, и наибольшей проблемой является распределение водных ресурсов. Сельское хозяйство в этом полупустынном регионе нуждается в ирригации и водоуправлении. Кыргызстан и Таджикистан владеют водохранилищами советских времен, от которых зависит сельское хозяйство стран, расположенных ниже по течению, - Узбекистана, Казахстана и Узбекистана. «Советская плановая экономика требовала от стран, находящихся выше по течению, собирать воду в своих плотинах и спускать ее вниз по течению в весенне-летний поливной период. Взамен этого страны, расположенные ниже по течению, богатые природным топливом (особенно газом, нефтью и углем), должны были поставлять вышерасположенным странам эти природные ископаемые, а также электричество, которого у тех не было», - объясняет Умида Хашимовав публикации «Central Asia-Caucasus Analyst».

Постсоветские государства с трудом пытаются договориться об условиях использования этих ресурсов, и ситуация еще более усложнилась, когда Узбекистан оставил региональную электрическую сеть в декабре 2009 года. По словам Эрики Марат из Джеймстаунского фонда, Узбекистан пользуется экспортом газа для оказания давления на вышерасположенные страны, назначая

«Исторически сложилось так, что землями Центральной Азии управляли самодержавные правители. Племенные и клановые связи по-прежнему играют значительную роль в политической, социальной и экономической жизни, однако, сейчас они эффективно используются для поддержания власти правящей элиты, а не для успешной мобилизации сколь бы то ни было значимой оппозиции».

— Евгений Бендерский
аналитик по делам евразийского региона

Этнические узбекские беженцы у киргизско-узбекской границы рядом с поселком Сураташ (июнь 2010 г). Узбекистан закрыл свои границы во избежание массового наплыва беженцев, спасающихся от стычек противоборствующих групп в Кыргызстане.

АГЕНТСТВО ФРАНС-ПРЕСС

цены, недоступные для его более бедных соседей. Чтобы избежать высоких издержек, Кыргызстан и Таджикистан хотят построить большее количество плотин ГЭС. Узбекистан решительно сопротивляется построению новых плотин, беспокоясь о нехватке воды в летний период. Казахстан взял на себя ведущую роль в содействии региональному сотрудничеству в области энергетики и поддержал растущую энергетическую независимость таджиков и киргизов и меры, принятые для строительства электросети, при необходимости, в обход Узбекистана. И если новое газовое месторождение в Таджикистане будет соответствовать ожиданиям, страна может стать энергетически независимой к концу 2011 года.

Энергетические богатства Казахстана, Туркменистана и Узбекистана предоставляют экономические возможности, которых нет у их более бедных соседей. Их энергоресурсы также подчеркивают важность установления стабильной и безопасной политической и экономической среды. Согласно публикации «World Politics Review», в этом регионе «содержится приблизительно 250 млрд. баррелей промышленных запасов нефти, плюс больше, чем 200 млрд. баррелей потенциальных запасов. Это не считая почти 328 триллионов кубических футов извлекаемого природного газа». Западная Европа надеется транспортировать обильные запасы центральноазиатского газа трубопроводом «Набукко», который пойдет в обход России и снизит зависимость Европы от российского поставщика газа «Газпрома».

АССОШИЭЙТЕД ПРЕСС

Житель Кыргызстана голосует на избирательном участке в г. Ош во время референдума по новой конституции в июне 2010 г. Всенародно утвержденная Конституция превратила Кыргызстан в первую парламентскую демократию в Центральной Азии.

Пока правительства стран Центральной Азии с недоверием относятся друг к другу, ИДУ и другие панисламистские экстремисты смотрят на весь регион как на свою территорию и пользуются отсутствием межгосударственного сотрудничества для проведения своих операций, невзирая на границы. ИДУ провело теракты в Узбекистане, Кыргызстане и Таджикистане. Уязвимостью границ пользуются и контрабандисты наркотиков. В докладе Управления ООН по наркотикам и преступности говорится, что отсутствие сотрудничества между центральноазиатскими правоохранительными органами препятствует борьбе с торговлей наркотиками: «Борьба с незаконным обращением наркотиков требует наличия хорошо организованных систем сбора, обработки и анализа информации, равно как и обмена окончательным информационным продуктом между задействованными на государственном и региональном уровне органами. К сожалению, недостатки сбора и обмена развединформацией продолжают препятствовать эффективному патрулированию границ между странами Центральной Азии и Афганистаном».

Вовлечение региона

Вопрос стабильности и безопасности в Центральной Азии может создать конфликт серьезные между государствами Запада. Как должны государства, решительно поддерживающие демократию, свободу и открытость, относиться к авторитарным режимам региона? Некоторые сторонники демократии полагают, что, поддерживая репрессивные, авторитарные режимы, Запад тем самым компрометирует себя, даже если стабильность, созданная этими режимами, обеспечивает рост торговли и инвестиций, сокращает обращение наркотиков и предупреждает распространение исламского экстремизма. Вторая точка зрения отдает предпочтение стратегии деятельного участия, согласно которой Запад предоставляет обучение и ресурсы правительствам Центральной Азии, тем самым способствуя демократическим реформам.

Некоторые считают, что либеральная демократия чужда культуре Центральной Азии. На сайте «Eurasianet». аналитик по делам евразийского региона Евгений Бендерский написал: «Исторически сложилось так, что землями Центральной Азии управляли самодержавные правители. Племенные и клановые связи по-

РИА Новости

Солдаты воздушно-штурмовой бригады Казахстана проводят развертывание после приземления в финальном этапе военных учений «Взаимодействие-2010», проведенных ОДКБ на полигоне «Чебаркуль» в России.

прежнему играют значительную роль в политической, социальной и экономической жизни, однако, сейчас они эффективно используются для поддержания власти правящей элиты, а не для успешной мобилизации сколь бы то ни было значимой оппозиции». Казахский политолог Марат Шибутов считает, что президент Нурсултан Назарбаев – это «единственное, на чем держится Казахстан», а граждане куда более обеспокоены вопросом энергетической безопасности, чем политическими свободами, пишет журнал «Der Spiegel». Тем не менее, некоторые утверждают, что, хотя авторитарное правление и может давать ощущение стабильности, эти режимы являются хрупкими и могут не выдержать сильного напора.

Признавая важность операций НАТО в Афганистане и постепенное превращение государств Центральной Азии в современные демократии, в ноябре 2010 года НАТО объявила о своих планах расширения сотрудничества в области безопасности. По данным «Eurasianet», количество оборудования и поставок, отправленных через Северную распределительную сеть, или СРС, значительно увеличится с транзитом 98% отгрузок через Узбекистан. Чиновники расхваливают улучшившиеся отношения и «продолжают содействовать узбекским властям в решении основных вопросов прав человека». По оценкам Министерства обороны США, СРС будет стимулировать экономический рост и «возможно, однажды соединит Центральную Азию с Индией, Пакистаном и другими ранее закрытыми рынками прямым наземным маршрутом через сердце Азии в сердце Европы».

Центральноазиатская безъядерная зона, или ЦАБЯЗ, является примером регионального сотрудничества и вовлеченности международного сообщества. Согласно подписанному в сентябре 2006 года соглашению, ЦАБЯЗ «является первой безъядерной зоной, полностью расположенной в северном полушарии», как заявило Международное агентство по атомной энергии. По данному соглашению, «в этой зоне запрещены разработка, производство, накапливание, закупка или владение любым ядерным взрывным устройством», и страны, его подписавшие, обязуются соответствовать национальным стандартам безопасности на ядерных объектах и выполнять положения Договора о всеобъемлющем запрещении ядерных испытаний, снижая риск контрабанды ядерного оружия. □

АГЕНТСТВО ФРАНС-ПРЕСС

Сторонники основателя WikiLeaks Джулиана Ассанжа в масках Гая Фокса во время демонстрации протеста против ареста Ассанжа, прошедшей в Амстердаме в декабре 2010 года. Члены группы хактивистов «Анонимы» используют это изображение Гая Фокса во время публичных акций.

«Хактивисты» наносят ответный удар

Кибернетические атаки на финансовые организации служат предупреждением

В декабре 2010 года сайты крупнейших международных платежных систем Visa, MasterCard и PayPal были на некоторое время выведены из строя, став жертвой скоординированной кибернетической атаки, названной ее организаторами операцией «Расплата». Эти сайты были атакованы «хактивистами», поддерживающими WikiLeaks и Джулиана Ассанжа, после того, как владеющие ими компании прекратили принимать пожертвования в пользу сайта WikiLeaks. Нанесенный данной атакой ущерб остается неизвестным, а ставшие ее жертвами компании заявили, что не понесли существенных убытков. Тем не менее, атакующие – называющие себя «Аноном» или «Анонимом» – продемонстрировали, что при помощи кибернетических атак можно проникнуть в компьютерные системы бизнес-структур и правительственных агентств и нарушить их работу.

Современная форма протеста

Протест Анонимов заключался не в скандировании лозунгов или в размахивании плакатами – их удар по тем, кого они считают врагами WikiLeaks, был выполнен в духе общего для Анонимов и для WikiLeaks виртуального мира. Созданный с целью предания гласности секретной и конфиденциальной информации о правительствах и корпорациях сайт WikiLeaks находится под давлением со стороны правительств США и других стран с тех пор, как в ноябре 2010 года сайт обнародовал более 250 тысяч дипломатических писем Государственного департамента США. По сообщению газеты «*The Independent*», США обвиняют WikiLeaks в том, что обнародование незаконно полученной правительственной информации подвергает опасности жизни людей, а также просят различные компании прекратить любое сотрудничество с сайтом.

Интернет-магазин Amazon, на чьих серверах размещался WikiLeaks, прекратил сотрудничество первым. За ним вскоре последовали Visa, MasterCard и PayPal, существенно сократив возможности WikiLeaks принимать добровольные финансовые пожертвования, поддерживающие работу сайта. Вскоре после этого начались кибернетические атаки.

Для своей атаки, развернувшейся в виртуальном мире, Анонимы использовали любимое оружие кибер-

нетических солдат: DDoS-атаки (распределенные атаки типа «отказ в обслуживании»). DDoS-атака заключается в перегрузке атакуемой компьютерной системы запросами, что делает невозможным доступ к ней для легитимных пользователей. Типичная DDoS-атака использует тысячи «скомпрометированных» компьютеров, обычно незаметно для пользователя зараженных вредоносными программами, позволяющими оператору дистанционно управлять зараженными компьютерами. Такие сети, или «ботнеты», широко используются преступными организациями. Кибернетические рэкетиры используют DDoS-атаки, вымогая у компаний «плату за защиту» наподобие того, как традиционные рэкетиры действуют в реальном мире.

Хактивисты, участвовавшие в операции «Расплата», создали добровольный ботнет. Как рассказал журналу «PC World» Ноа Бар-Йоссеф, специалист по безопасности из компании Imperva, занимающейся обеспечением безопасности данных, хактивисты привлекали к созданию ботнета людей из своей среды, прося их добровольно загрузить на свои компьютеры вредоносные программы, – в результате отпала необходимость заражать компьютеры посторонних людей. По информации посвященного современным технологиям журнала «Fast Company», для планирования атак, общения и координации своих действий хактивисты пользовались Твиттером и другими подобными сайтами.

> «Потребители и налогоплательщики могут этого и не осознавать, но растущая угроза кибернетических атак, компьютерных вирусов и кражи персональных данных на самом деле обходится им в миллиарды долларов».
>
> — Генри Трак, колумнист сайта www.GoBankingRates.com, пишущий о личных финансах.

По иронии судьбы, сам сайт WikiLeaks также стал жертвой DDoS-атаки. Хакер, известный под ником «Шут» (The Jester) и называющий себя «хактивистом добра», атаковал сайт WikiLeaks в ноябре 2010 года, обвалив его на короткое время, до того, как на нем были опубликованы сотни тысяч секретных дипломатических телеграмм. Как говорится в показанном по Си-Эн-Эн сюжете, «Шут» атаковал сайты, содержащие «онлайн-подстрекательство молодых мусульман к осуществлению насильственных деяний во имя джихада». Он рассказал Си-Эн-Эн, что выступает против WikiLeaks за «попытку подвергнуть опасности жизни наших солдат, другие объекты, а также наши отношения с другими странами».

Насколько результативными были действия хактивистов?

По данным ББС, атакованные Анонимами сайты испытали перебои в работе, но атаки на платежные системы не повлияли на обработку транзакций по кредитным картам. Представители MasterCard признали, что некоторые онлайн-сервисы работали с перебоями, но ни обработка транзакций по картам, ни конфиденциальность данных владельцев карт не пострадали. Тед Карр, представитель Visa, сказал ББС, что система обработки транзакций по картам продолжала нормальную работу. Анонимы сначала сообщили о предстоящей атаке на Amazon, но затем выбрали PayPal в качестве новой цели этой атаки. Представители этой электронной платежной системы сообщили, что блог компании был выведен из строя, но что обработка транзакций продолжалась, хотя и медленнее, чем обычно.

Другие атаки оказались более успешными. В новостях сообщалось, что швейцарский банк PostFinance испытывал перебои в работе в течение десяти часов, а сайт шведских обвинителей по делу против Ассанжа о преступлениях сексуального характера был выведен из строя на несколько часов.

Самыми крупными целями Анонимов были Visa, MasterCard, PayPal и Amazon. Так, Visa и MasterCard являются двумя крупнейшими в мире платежными системами для потребителей; в 2010 году заявленная ими выручка составила 8 и 5,5 миллиардов долларов соответственно. PayPal, принадлежащая работающей в области интернет-аукционов компании eBay, объявила, что ее выручка за 2010 год составила почти 2,8 миллиарда долларов. Ничто не указывает на то, что DDoS-атаки нанесли компаниям, против которых были направлены, значительный финансовый ущерб; по сути они свелись к виртуальным граффити в онлайн-«приемных» банков.

Последствия

После проведенных сторонниками WikiLeaks атак правоохранительные органы арестовали нескольких человек. Пять хактивистов из числа Анонимов были арестованы в Лондоне в январе 2011 года, хотя лондонская полиция и отказалась комментировать их причастность к атакам. Двое хакеров-подростков были арестованы в Нидерландах в декабре 2010 года. По состоянию на начало 2011 года, полиция в Европе и Северной Америке продолжает выдавать ордера на арест подозреваемых, причастных к этим незаконным кибернетическим атакам.

И хотя эти недавние атаки были по большей части безуспешными, они привлекли внимание к тому факту, что преступники и террористы могут вызвать крупномасштабные финансовые проблемы и обнародовать конфиденциальные данные кредитных организаций. По оценкам британских должностных лиц, интернет-атаки и вирусы обходятся мировой экономике в 86 миллиардов долларов в год – сумма, которую в конечном итоге платят потребители и налогоплательщики. Обеспечение безопасности финансовых организаций и других жизненно важных объектов гражданской инфраструктуры будет, без сомнения, оставаться дорогостоящей задачей. □

Многонациональная Европа

Интеграция меньшинств может пойти на пользу всем

В июле 2010 года в небольшой деревне Сент-Эньян полицейский национальной жандармерии Франции выстрелил и убил мужчину, принадлежащего к этническому меньшинству рома. По версии полиции, мужчина состоял в розыске по обвинению в краже и промчался через два полицейских контрольно-пропускных пункта, ранив полицейского. Два дня спустя десятки рома, проживающих в близлежащем лагере, вооружившись топорами, ножами и железными прутьями, напали на местный участок полиции и устроили беспорядки на улицах города. Служба новостей ББС сообщила, что в результате президент Франции Николя Саркози «обещал, что ответственные за беспорядки и насилие будут «сурово наказаны»» и приказал уничтожить сотни нелегальных лагерей рома, а проживающих в них людей депортировать в страны их первоначального пребывания. В тот же день во французском городе Гренобле мусульманская молодежь устроила мятеж, после того как подозреваемый в вооруженном ограблении выходец из Северной Африки был убит в перестрелке с полицией.

АГЕНТСТВО ФРАНС-ПРЕСС

Принятые Саркози меры были направлены на установление более жесткого правопорядка и стали ответом на возрастающее беспокойство французского общества, озабоченного увеличением беспорядков и насилия в общинах рома и других этнических меньшинств. Однако результат оказался совершенно иным. Эти меры инициировали острую общеевропейскую дискуссию о правах меньшинств и интеграции этнических меньшинств – дискуссию, которую пора было начать уже давно, как считают многие в Европе, включая и группы, борющиеся за защиту гражданских прав и против дискриминации рома. Как сказала в интервью ББС Тара Бедард из Европейского центра по правам рома: «Кампания Саркози наконец-то поместила проблемы рома «в самый центр повестки дня Европы»». Однако эта дискуссия актуальна не только для общин рома, но и для растущих общин мусульманских иммигрантов из Центральной Азии, Ближнего Востока и Северной Африки.

Полиэтническая Европа

Первые рома индийского происхождения прибыли в Европу не позднее 14 века и были широко известны как цыгане (Gypsy), потому что тогда было распространено ошибочное мнение, что они родом из Египта. Современное население рома в Европе составляет приблизительно 11 - 16 миллионов и является самым большим и быстро растущим этническим меньшинством на континенте. Веками цыгане народности рома подвергались дискриминации и эксплуатации на разных уровнях. Дискриминация местным населением, усугубляемая кочевым образом жизни рома, их замкнутой и ориентированной на себя культурой, приводила к взаимному недоверию и страху между рома и населением стран, где они жили. Сегодня европейские рома по-прежнему страдают от высокой безработицы, широко распространенной неграмотности и бедности.

Рома представляют довольно необычный пример неудачной культурной интеграции или отказа от нее. По мнению Искры Узуновой («Arizona Journal of International & Comparative Law»), крайне важно понять положение этого этнического меньшинства в Европе и историю взаимоотношений рома с доминирующими культурами, чтобы «выработать эффективные пути решения глубоких социальных, политических и культурных проблем и трудностей, с которыми рома сталкиваются в Европе». Такое понимание также может принести пользу и в разработке единой европейской политики в области прав меньшинств и интеграции иммигрантов, недавно прибывших из Азии и Африки.

Современная волна иммиграции началась, когда европейские страны, восстанавливаясь после Второй мировой войны,

Лагерь рома в Вильнев-д'Аск во Франции — ребенок ест, сидя на руках у женщины, через день после их депортации из другого лагеря. Комитет ООН по борьбе с расизмом убеждал Францию «избегать» массовых депортаций рома.

Дети рома и румын вместе обучаются в Даррвари, Румыния. Дети рома страдают от сегрегации и дискриминации в сфере образования во многих европейских странах.

АГЕНТСТВО ФРАНС-ПРЕСС

АГЕНТСТВО ФРАНС-ПРЕСС

Имамы посещают службу в честь торжественного открытия новой мечети Омара в районе Кройцберг в Берлине во время торжественного открытия исламского центра Машари. Мусульманское население Европы быстро увеличивается.

Озлем Джекидж недавно избранный член Фолькетинга, датского парламента, со своей новорожденной дочерью в Копенгагене. Джекидж и Йилдиз Акдоган, первые за всю историю датского парламента женщины-мусульманки.

РЕЙТЕР

начали компенсировать мигрантами нехватку рабочей силы. Эти мигранты, как и рома, приносили с собой свои особенности культуры, языки, религии, которые существенно отличались от исконно европейских. Многие иммигранты из Азии и Африки были мусульманами. Первая волна иммиграции шла, главным образом, из бывших европейских колоний: жители Пакистана и Бангладеш ехали в Великобританию, жители Алжира во Францию. Германия и Нидерланды привлекли большое количество мигрантов-мусульман из Турции и Индонезии. По словам Оливьера Роя из Французского национального центра научных исследований, большинство ранних иммигрантов приезжали по экономическим мотивам и не собирались оставаться, они «не идентифицировали себя как западные или европейские мусульмане». Для первого поколения мигрантов проблема интеграции не была актуальной, но второе и третье поколения «хотят здесь остаться», – сказал Рой.

Иммигранты обычно склонны селиться и жить вместе со своими соотечественниками и даже выходцами из того же города. Так они пытаются воссоздать социальные сети и структуры поддержки, типичные для родной страны. Эстер Бен-Давид из журнала «Middle East Quarterly» утверждает, что эта «динамика иммиграции» ограничивает взаимодействие мигрантов с другими членами общества, что приводит к созданию замкнутых сообществ, препятствующих культурной интеграции. В этом отношении мусульманские иммигранты частично напоминают рома, которые сохранили «этноцентрическую» позицию и отделились от доминирующей европейской культуры. Хотя такая самоизоляция и помогает приезжим приспособиться к жизни в Европе и ограждает их от дискриминации, в то же время любая сегрегация – добровольная или принудительная – препятствует кросс-культурному пониманию и может усиливать предрассудки и дискриминацию.

Сегрегация, дискриминация, радикализация

Согласно «Стратегии Евросоюза против радикализма», опубликованной в ноябре 2008 года, политические и культурные факторы сильнее всего влияют на процесс радикализации европейских мигрантов-мусульман. Решающую роль играет их слабое политическое представительство. В результате «отсутствия политических перспектив» появляется ощущение, что выразить недовольство можно только неполитическими средствами. Этот документ также указывает на «сложное положение в области трудоустройства, образования и условий проживания, а также негативные стереотипы и предрассудки». Это ведет к отчуждению и росту привязанности к родной культуре и религии, а возможно, и к их искаженному пониманию. Подготовленный Рутгерским университетом отчет «Интеграция и безопасность: мусульманские меньшинства и государственная политика в Европе и США» утверждает, что меры безопасности, введенные после событий 11 сентября 2001 года, стали препятствием в процессе интеграции мусульманских иммигрантов и привели к усилению дискриминации и отчуждения. «На самом деле, доведенные до крайности меры безопасности имели противоположный эффект и привели к парадоксу: усиление мер безопасности влечет за собой еще большую радикализацию».

Этническая и культурная изоляция также ограничивает экономические возможности. Николета Попкостадинова в журнале «Eurozine» пишет, что даже до мировой рецессии уровень безработицы рома в Центральной и Восточной Европе по официальной статистике варьировался от 50 до 75%. Эти данные также свидетельствуют о том, что рома продолжают сталкиваться с дискриминацией, потому что уровень безработицы рома в три раза превышает общий уровень безработицы остального населения Европы даже с учетом уровня образования. Рома также страдают от дискриминации и в области образования, что еще больше обостряет проблему. Попкостадинова сообщает, что в Болгарии «политика сегрегации лишила целые поколения рома шанса приблизиться к равноправному участию на рынке труда».

Провал интеграции имеет свою цену, которую платят не только дискриминируемые меньшинства, но и все общество. Когда таланты целой группы людей оказываются невостребованы экономикой, страдает производительность труда. Конкуренция уменьшается, возникает потенциальная нехватка квалифицированной рабочей силы, что, в свою очередь, ведет к снижению производительности и ВВП. Болгарские экономисты Лачезар Богданов и Георгий Ангелов подготовили отчет, в котором они доказывают, что рома– это еще неиспользованные, скрытые ресурсы экономического потенциала, и поэтому необходимо инвестировать деньги в их образование и профессиональное обучение.

Экономический потенциал мусульманской общины также недооценен. Беспорядки 2005 года во французских мусульманских кварталах были в основном спровоцированы высоким уровнем безработицы среди мусульманской молодежи. Вышедший в 2005 году доклад научно-исследовательской службы конгресса, посвященный проблеме интеграции европейских мусульман, подчеркивает, что уровень безработицы мусульман может в три раза превышать безработицу среди населения в целом. Такая разница в статистических показателях свидетельствует о наличии дискриминации. Бельгийский предприниматель Имэйн Карич в своем отчете, подготовленном для Центра Европейских политических исследований, сделала акцент на том, что мусульмане переселились в Европу, преследуя экономические цели и возможности. «Исламский характер придает особое значение важности образования, доверия и усердной работе как основным компонентам экономического развития», – сказала она.

Движение вперед

Европа продолжает работать над созданием разнородных

интегрированных сообществ, в том числе рома, мусульман и других этнических меньшинств. В 2008 году Европейский совет разработал программу «Многокультурные города» с целью «управления этническим и социо-культурным многообразием» во все более многообразной Европе. Программа, основанная на предпосылке, что «успешные города и общества будущего будут многокультурными», начала работать в 11 городах, которые должны сформировать стратегии межкультурной интеграции.

Несмотря на то, что процесс интеграции очень неоднороден, примеры успеха множатся. Мусульмане были избраны в парламенты Великобритании, Нидерландов, Дании, Франции и Германии. После выборов 2009 года в состав парламента Европейского союза вошли 11 мусульман. Центр Европейских политических исследований сообщает, что мусульмане все больше преуспевают в бизнесе и университетах, чему способствует совет мусульман по сотрудничеству в Европе при Европейском союзе.

Западноевропейские нации, борющиеся с большими миграционными потоками рома, пребывающими из Восточной Европы, призвали Румынию и Болгарию приложить больше усилий для интеграции своих граждан - рома по национальности. Недавно вошедшие в Европейский союз страны, к которым присоединяются общественные организации и защитники прав рома, берут пример с Европейского союза в создании всеобъемлющей стратегии интеграции рома. Госсекретарь Португалии по европейским вопросам Педро Луртье дает следующее объяснение: «Поскольку эта проблема касается не одной нации, Европейский союз должен играть роль в интеграции этих групп населения».

Отчет Богданова и Ангелова призывает к более инновационному и активному подходу. Они предлагают сделать акцент на профессиональной подготовке, а не системе социальных пособий, и поддержать «краткосрочные увеличения издержек государства с целью ускорения мобилизации населения рома и их трансформации в рабочую силу». Румын Гелу Доменика соглашается с таким подходом: «Мы должны поменять наш дискурс защиты прав человека на основания для инвестирования в общины рома. Мы должны помочь государству осознать, что проще и дешевле найти трудовые ресурсы в общине рома, чем привезти рабочих-мигрантов из-за рубежа».

Образование – ключ к новым возможностям

Успешная интеграция этнических меньшинств зависит от систем образования, которые не всегда обращались с мусульманами и рома как с равными. Совместный доклад Организации по безопасности и сотрудничеству в Европе и Совета Европы по проблемам миграции рома ссылается на: «большую неуспеваемость детей рома в школе и сохранение школьной неуспеваемости в следующих поколениях, из-за практики сегрегированных образовательных учреждений, произвольных отказов принимать в школы детей рома и других подобных практик». В докладе ЕС «Мусульмане в Европейском союзе: дискриминация и исламофобия» от 2006 года утверждается, что дети из этнических меньшинств часто демонстрируют более низкую успеваемость и с более высокой вероятностью не закончат школу.

Однако процесс интеграции – это процесс двусторонний. Многие рома, особенно в Центральной и Восточной Европе, традиционно разделяют глубоко укоренившееся культурное недоверие к системе формального образования. Это недоверие способствует неграмотности и бедности. Джейк Бауэрс, британский журналист, рома по происхождению, указывает на тот факт, что рома традиционно мало ценили формальное образование, предпочитая ему свободу самообразования и фрилансерства. «Образование остается противоречивой необходимостью для многих рома пишет Бауэрс на сайте «Travellers Times Online». «Оно ценится только как способ научиться читать и писать, но ему не доверяют из-за «культурного загрязнения», которое привносится в процесс обучения».

Некоторые европейские мусульмане также считают государственное образование культурной угрозой. Исследование Хольгера Дауна и Рэза Арджманда в «Review of Education» продемонстрировало, что «часто родители, иммигрировавшие из преимущественно мусульманских стран, не уверены, что новая страна даст им достаточно возможностей воспитать детей в духе мусульманских ценностей и норм. Для многих таких родителей мусульманское моральное воспитание крайне важно, независимо от того, имеет ли оно место в рамках системы формального образования или в условиях неформальной социализации».

В 2010-2011 гг. главы европейских стран, прежде всего Великобритании и Германии, несколько раз подчеркивали, что образование и обучение рабочим специальностям даст новые возможности мусульманским и цыганским общинам в Европе и позволит им реализовать свой экономический потенциал. Однако для того чтобы реализовать и сполна использовать возможности Европы, этнические меньшинства должны освоиться в обществе, в котором они проживают. Европейская программа, успешно объединяющая исторически изолированные этнические группы, такие как рома, может стать образцом для интеграции других иммигрантских групп, таким образом, сокращая культурное отчуждение, которое может привести к радикализации, и создавая более продуктивные и преуспевающие межкультурные сообщества. Как заявил премьер-министр Великобритании Дэвид Кэмерон в своем обращении к участникам Мюнхенской конференции по вопросам безопасности, проводимой в феврале 2011 года, многие европейские страны, выбравшие путь «государственного мультикультурализма», невольно провели разделение своих граждан по религиозному и этническому принципу. «Вместо того, чтобы поощрять народ жить раздельно, - заявил Кэмерон, - мы должны создать четкое ощущение общей национальной целостности и открытости для всех». □

«Кибернетическая война: взляд изнутри»

Книга Джеффри Карра
Г. Себастопол (Калифорния, США): O'Reilly Media, 2009; 240 стр.

Обзор представлен подп-ком Джо Мэттьюзом,
управляющим редактором журнала «*per Concordiam*»

Джеффри Карр использует свой богатый опыт и знание кибернетической войны для создания сборника статей в одной познавательной книге «Кибернетическая вой-на: взгляд изнутри». Карр – эксперт в вопросах кибербезопасности и директор американской компании «GreyLogic», занимающейся вопросами компьютерной безопасности. Он специализируется на расследованиях кибернетических атак. В своей книге он кратко касается всех важных вопросов, стоящих перед государствами, пытающимися защитить важные данные, при этом упрощая обмен информацией. Его книга - попытка кратко рассказать высшим должностным лицам и сотрудникам служб безопасности о задачах и трудностях защиты кибернетического пространства. Эта книга легко читается теми, кто тесно связан с этими вопросами, а для обычных пользователей кибернетического пространства, желающих глубже понять проблемы безопасности, она является познавательным чтением.

В книге просто и прямо указывается на одну из самых крупных проблем для руководства относительно кибернетической безопасности: в мире не существует общего определения того, что такое кибернетическая атака. Примеры недавних кибернетических атак и идея о том, что государства могут вести «войну идей» в кибернетическом пространстве, в поисках победы без человеческих жертв, являются убедительной картиной возможного будущего. В книге также содержится очень подробное описание роста «негосударственных» хакеров.

Из наиболее актуальных проблем в книге обсуждаются юридический статус кибернетической войны и ее определение. Помимо неясности статуса, существует также необходимость усиления сотрудничества полицейских сил и укрепления курса в отношении незаконной деятельности в кибернетическом пространстве. Расследование киберпреступлений и выявление преступников - еще одна сложность. Анонимность в кибернетическом пространстве – одна из основных причин процветания организованной преступности в виртуальном мире. В книге приведены подробные примеры того, как преступные организации и «негосударственные» хакеры анонимно действуют в Интернете.

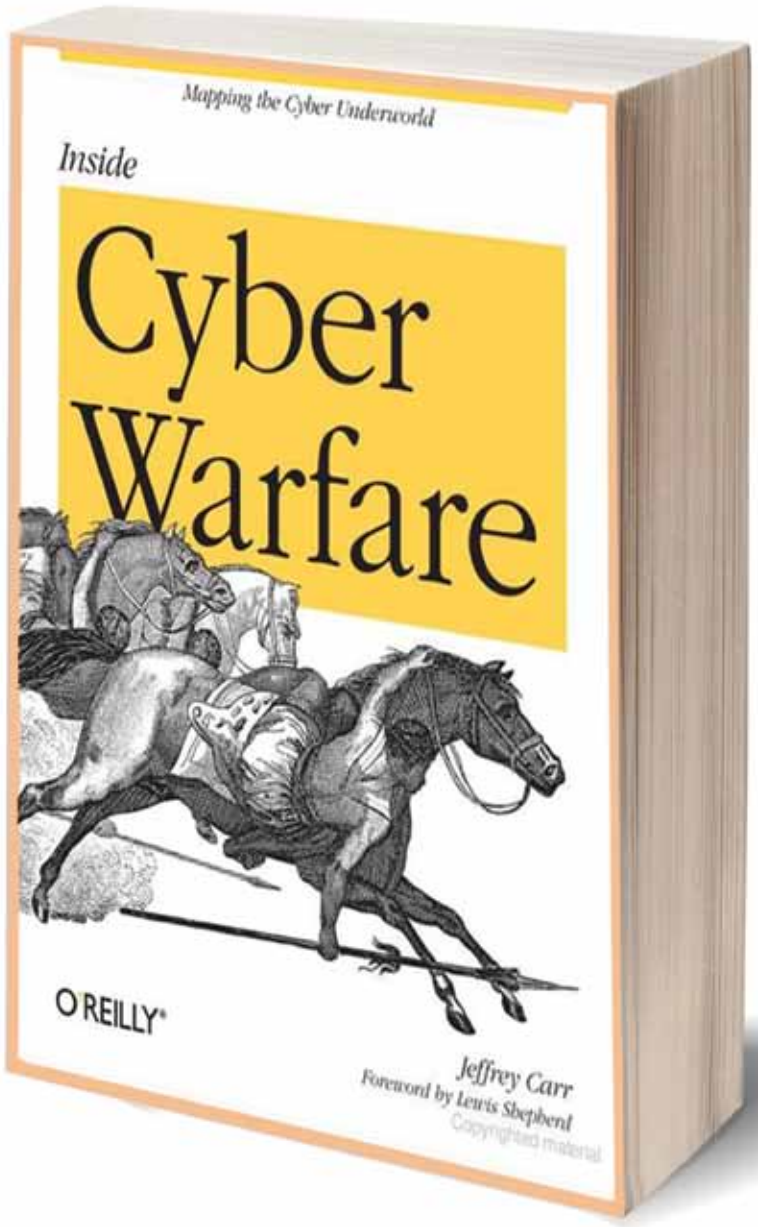
В главе о «негосударственных» хакерах и социальной сети убедительно рассказывается о силе социальных медиа в стимулировании политической поддержки. Сегодня Интернет –

> “В книге приведены подробные примеры того, как преступные организации и «негосударственные» хакеры анонимно действуют в Интернете.”

это средство получения информации, повышения уровня образования и возможность заручиться поддержкой социальных действий. Этот беспрецедентный объем коммуникации способствует передаче ложных данных. Предоставление под маской достоверности фальсифицированной информации является попыткой повлиять на определенную часть общества или государства.

Если у читателя есть время на чтение только одной главы, следует прочесть главу о кибернетической модели раннего оповещения. Эта глава написана Недом Мораном, старшим разведчиком-аналитиком и адъюнкт-профессором в области разведисследований в Джорджтаунском университете в Вашингтоне. Моран описывает создание аналитической основы для прогнозирования возможных политически мотивированных кибернетических атак. Для этого он использует три практических примера. Более точный метод прогноза определения источника возможной кибернетической атаки может значительно улучшить возможности развивающихся в стране центров национальной кибернетической безопасности.

Высшим должностным лицам стоит прочесть книгу «Кибернетическая война: взгляд изнутри» хотя бы из-за последней ее главы. В этой главе собраны рекомендации сборника статей обо всем, вплоть до изменений в политике, изменений в операционной системе и привлечении к ответственности провайдеров сервисов и интернет-хостинга за незаконную деятельность. Одна из таких рекомендаций – переход от операционной системы Microsoft Windows к системе Red Hat Linux с целью уничтожения большинства зловредных программ. Еще одна рекомендация предлагает переход к политике активной обороны информационных систем и общенациональному подходу к кибернетической безопасности. Это полезный совет для тех, кто уполномочен начать изменения. □



Заявление об ограничении ответственности: взгляды и выводы, изложенные в обзоре данной книги, являются мнением автора и не обязательно представляют официальную политику или утверждения, высказанные или подразумеваемые, правительства США.

Стационарные курсы

Democratia per fidem et concordiam

Демократия через доверие и дружбу

Отдел регистрации
George C. Marshall Center
Gernackerstrasse 2
82467 Garmisch-Partenkirchen
Germany

Телефон: +49-8821-750-2656
Факс: +49-8821-750-2650

www.marshallcenter.org
registrar@marshallcenter.org

Порядок регистрации
Европейский центр исследований по вопросам безопасности имени Джорджа К. Маршалла не принимает заявлений напрямую. Заявления на все курсы должны поступать через соответствующее министерство и посольства США или ФРГ в стране проживания кандидата. Тем не менее, отдел регистрации слушателей готов помочь кандидатам в проведении процедуры. Запрос можно направить по электронному адресу: registrar@marshallcenter.org

ПРОГРАММА «ТЕРРОРИЗМ И ВОПРОСЫ БЕЗОПАСНОСТИ» (ПТВБ)

Эта пятинедельная программа, проводимая два раза в год, раскрывает многоплановые аспекты угрозы терроризма для разных стран и адресована представителям среднего и высшего руководящего звена правительственных органов, силовых и правоохранительных структур, а также контртеррористических организаций. ПТВБ сосредотачивает внимание на борьбе с терроризмом и одновременном сохранении приверженности основополагающим ценностям демократического общества. Курс состоит из пяти разделов: исторический и теоретический обзор терроризма, уязвимость террористических групп, роль законодательства, финансирование террористической деятельности и сотрудничество в области безопасности.

ПТВБ 12-3

10 февраля – 16 марта 2012

(прием заявок до 16 декабря 2011)

Февраль

ВС	ПН	ВТ	СР	ЧТ	ПТ	СБ
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29			

Март

ВС	ПН	ВТ	СР	ЧТ	ПТ	СБ
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

ПРОГРАММА УГЛУБЛЕННОГО ИЗУЧЕНИЯ ВОПРОСОВ БЕЗОПАСНОСТИ (ПАСС)

Основной курс Центра имени Маршалла проводится два раза в год и продолжается три месяца. Эта интенсивная и интеллектуально насыщенная программа обеспечивает вузовский уровень подготовки специалистов по проблемам политики безопасности, оборонного комплекса и международных отношений, а также по другим смежным дисциплинам. Программа предусматривает ознакомление с аналитическими и информационными материалами, участие в работе семинаров, полемике, дискуссиях за круглым столом, ролевых играх и учебно-ознакомительных поездках. Слушатели дожны владеть одним из трех языков, на которых читается курс этой программы: английским, немецким или русским.

ПАСС 12-5

23 марта – 31 мая 2012

(прием заявок до 27 января 2012)

Март

ВС	ПН	ВТ	СР	ЧТ	ПТ	СБ
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Апрель

ВС	ПН	ВТ	СР	ЧТ	ПТ	СБ
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

Май

ВС	ПН	ВТ	СР	ЧТ	ПТ	СБ
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

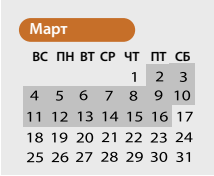
«БОРЬБА С ОРУЖИЕМ МАССОВОГО ПОРАЖЕНИЯ/ ТЕРРОРИЗМОМ» (СБОМП/Т)

Данный двухнедельный семинар для профессионалов в области национальной безопасности проводит всесторонний анализ основ противодействия распространению оружия массового поражения (ОМУ), а также задач и сложностей, связанных с угрозой химического, биологического, радиологического и ядерного характера (CBRN).

СБОМП/Т 12-4

2-16 марта 2012

(прием заявок до 6 января 2012)



СЕМИНАР «ТРАНСАТЛАНТИЧЕСКАЯ ГРАЖДАНСКАЯ БЕЗОПАСНОСТЬ» (СТАКС)

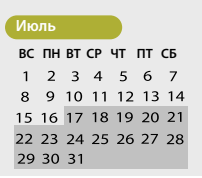
Этот семинар проводится два раза в год и продолжается три недели. В ходе семинара гражданские специалисты в области безопасности из Европы, Евразии и Северной Америки получают возможность углубить знания об эффективных методах и путях решения проблем внутренней безопасности, имеющих региональное и международное значение. Программа состоит из четырех разделов – угрозы и факторы риска, подготовка и защита, ответные меры и ликвидация последствий и учебная поездка – и направлена на углубление основных знаний и навыков.

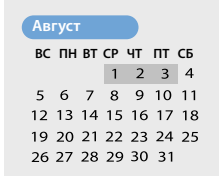
СТАКС 12-7

17 июля

3 августа 2012

(прием заявок до 22 мая 2011)





СЕМИНАР ДЛЯ ВЫСШЕГО РУКОВОДЯЩЕГО СОСТАВА (СВРС)

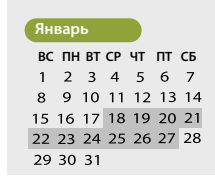
Семинар является форумом, который позволяет проводить углубленное изучение вопросов международной безопасности. В зимнем и осеннем семинарах участвуют высокопоставленные правительственные чиновники, генералы и адмиралы, послы и другие высокопоставленные дипломатические работники, министры, заместители министров, парламентарии. Формат СВРС предусматривает выступления высокопоставленных должностных лиц и признанных экспертов, а также дискуссии по прослушанным лекциям в составе семинарских групп. Основной темой занятий на СВРС в 2010 году станут общие вопросы незаконного оборота наркотиков и терроризма и их влияния на безопасность в Европе и за ее пределами.

СВРС 12-1

18-27 января 2012

(прием заявок до 22 ноября 2011)

События в Странах Северной Африки и Ближнего Восток - Значение для Европы и Евразии



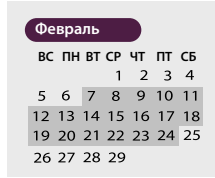
СТАБИЛЬНОСТЬ, БЕЗОПАСНОСТЬ, ПЕРЕХОД И ВОССТАНОВЛЕНИЕ (ССТаР)

Данный курс продолжительностью три недели проводится два раза в год. В программе рассматриваются вопросы о том, с какой целью и когда необходимо проводить операции по обеспечению стабильности, безопасности, перехода и восстановления с учетом глобальной ситуации с точки зрения безопасности и как обеспечить продуктивное участие в таких операциях разных стран. Программа состоит из четырех частей, которые направлены на основные проблемы ССТР, основополагающие организационные и оперативные требования, выполнение которых обеспечивает успешность таких операций, и находящиеся в распоряжении стран-участниц ресурсы для укрепления соответствующего потенциала.

ССТаР 12-2

7-24 февраля 2012

(прием заявок до 13 декабря 2011)



СЛУЖБА ПОДДЕРЖКИ ВЫПУСКНИКОВ

Дин Двигенс, начальник
тел +49 8821 750 2378
dwigansd@marshallcenter.org

Барбара Уизер
Албания, Болгария, Босния и Герцеговина, Греция, Косово, Македония, Румыния, Сербия, Словения, Турция, Хорватия, Черногория

Языки: английский, русский, немецкий

тел + 49 (0) 8821-750-2291
witherb@marshallcenter.org
Здание 102, комната 206 B

Крис О'Коннор
Беларусь, Венгрия, Латвия, Литва, Молдова, Польша, Словакия, Украина, Чехия, Эстония

Языки: английский, русский, польский

тел + 49 (0) 8821-750-2706
oconnorc@marshallcenter.org
Здание 102, комната 205

Мила Бэквит
Азербайджан, Армения, Афганистан, Грузия, Казахстан, Кыргызстан, Монголия, Пакистан, Таджикистан, Туркменистан, Узбекистан

Языки: английский, немецкий, русский

тел + 49 (0) 8821-750-2014
ludmilla.beckwith@marshallcenter.org
Здание 102, комната 206 A

Франк Бэр
Германия, Австрия, Швейцария

Языки: немецкий, английский, баварский

тел + 49 (0) 8821-750-2814
frank.baer@marshallcenter.org
здание 102, комната 217

Рэнди Карпинэн
Африка, Ближний восток, Западная Европа, Россия, Северная и Южная Америка, Южная и юго-восточная Азия

Языки: английский, испанский, немецкий, русский, финский

тел + 49 (0) 8821-750-2112
karpinenr@marshallcenter.org
Здание 102, комната 219

mcalumni@marshallcenter.org

Подать материал для публикации

Вы заинтересованы в подаче материалов для публикации в журнале *per Concordiam*? Правила подачи материалов для публикации можно найти по адресу **http://tinyurl.com/per-concordiam-submissions**

Подписаться

Если Вы хотите подписаться на **БЕСПЛАТНУЮ** доставку журнала *per Concordiam*, пожалуйста, свяжитесь с нами по электронной почте **editor@perconcordiam.org**

Найти нас

Вы можете найти *per Concordiam* в интернете по адресу:
Центр Маршалла: **http://tinyurl.com/per-concordiam-magazine**
Twitter: **www.twitter.com/per_concordiam**
Facebook: **http://tinyurl.com/perConcordiam-Facebook**
Информационный портал ЦИМ: **https://members.marshallcenter.org**
Отдел по работе с выпускниками: **mcalumni@marshallcenter.org**

ФОТОГРАФИЯ ПРЕДОСТАВЛЕНА ЦЕНТРОМ МАРШАЛЛА

Европейский центр исследований по вопросам безопасности имени Джорджа К. Маршалла в Гармиш-Партенкирхене, Германия.