Плавание в киберморе

Джеймс Ставридис

адмирал, командующий Европейского командования США и Верховный главнокомандующий ОВС НАТО в Европе.

Элтон С. Паркер III

военный помощник Вице-президента по академическим вопросам в Национальном Университете Обороны США.

Карьера в морской профессии приносит ясность в бурные и неопределенные воды морей и океанов. Чтобы успешно ориентироваться в этих водах, необходимо постоянное изучение, понимание и применение на международном уровне набора стандартов и норм, известных как правила дорожного движения. Есть «правила», которые применяются ко всем «глобальным уровням» — тому, что мы в Минобороны классифицировали как домены, а именно земля, море, воздух, космос и, соответственно, привыкли к их существованию и навигации в пределах границ, не нарушая установленные рамки.

Существует еще одна область, которая подвергается такой же классификации и определению. Она похожа на море в ее чистой величине, кажущейся вездесущности и смертельном потенциале, но она также уникальная в том, что не состоит из воды и волн; скорее, она состоит из нулей и единиц, оптических волокон и фотонов, маршрутизаторов и браузеров, спутников и серверов. Это, конечно, киберпространство, новое всеобщее достояние, среда, называемая у нас киберморем. В нем мы отправляемся в плавание каждый день в компании миллиардов других путешественников — многие начинают вояж с явно пересекающимися целями. Вместе мы включаем наши нетбуки и планшеты, берем наши смартфоны и используем обширный набор портов (и порталов) для подключения к остальному миру со скоростью мысли со всех видов различных судов, транспортных средств и ремесел.

Неограниченный потенциал

Киберморе является высшим выражением свободы, так как оно не может быть ограничено национальными или международными границами, нарисованными на любой карте или схеме, которые влияют лишь в редких случаях. Как и в дни фронтира в каждом новом домене, потенциал там безграничен, но

поскольку реалии человеческой экспансии, коммерции и взаимодействие обычно опережают политику и правила, как было во времена Дикого Запада и ранних мореходных экспедиций, преступное поведение изобилует, а потенциал для пиратства, нападений и конфликта всегда маячит за горизонтом. Чтобы подчеркнуть это, вспомним детство Интернета, когда он состоял только из несколько серверов и узлов, подключенных к устройствам, которые имели меньшую скорость вычислений и мощность, чем сегодняшние цифровые часы, так что было относительно легко регулировать движение. Но в начале 1990-х гг., однако, появились миллионы устройств, подключенных к сети Интернет, и в 2011 г. мы превзошли один миллиард устройств, связывающих нас по всему миру. Никогда раньше информационный обмен не был так легок и так потенциально разрушителен... И это только сегодня.

Эволюция завтрашнего дня обещает еще большую мобильность с помощью более быстрых, более компактных и более умных устройств. По мере роста, изменений и развития этого домена растет и наша зависимость от него. Мы продолжаем находить новые способы по обеспечению доступности, создаем новые формы человеческого взаимодействия, что делает нас ближе друг к другу, по крайней мере, виртуально. Будь то электронная почта, обмен мгновенными сообщениями, чат, твиттер, блоги, социальные сети, розничная продажа или взаимодействие в бизнесе, военные организации, члены правительства, неправительственные организации, частные и государственные предприятия каждый день плавают в диком киберморе.

В военной сфере, когда мы говорим о кибердомене, легко и соблазнительно свести обсуждение только к кибервойне или кибератаке. Хотя они являются важными элементами для разговора, сама тема гораздо шире, поэтому обсуждение дел также должно быть значительно шире. Мы живем во все более взаимосвязанном мире, конкурентном рынке, где основным товаром являются именно идеи, а цикл новостей 24/7 с почти мгновенной отчетностью широко распространяет истории. Это изобильный, бурный, и изнурительный рынок, и все мы должны продолжать конкурировать за нашу «долю» на этом рынке. В этом мире информация является властью, и эта власть увеличивается в геометрической прогрессии когда она совместна.

Мы должны принять традиционные формы обмена (интервью для прессы, газеты, печатные журналы и т. д.), а затем объединить их с новыми формами, такими как блоги, твиттер и размещения в Facebook. В качестве примера можно привести посты в Facebook и твиттер Верховного главнокомандующего ОВС НАТО в Европе, которых было около 13000, а блог Европейского командования США (USEUCOM) был просмотрен более 185 000 раз за последние два года. Но эти цифры бледнеют в сравнении с потенциалом соединений, который существует в этой еще огромной и дикой области. Например, Facebook превысил Google

в еженедельном трафике в Соединенных Штатах; Леди Гага и Джастин Бибер имеют больше последователей в Твиттер, чем все население Зимбабве, Кубы, Бельгии, Греции, Португалии или Швеция — там более 200 млн. общественных блогов.

Кроме того, радио понадобилось примерно 38 лет, чтобы достичь аудитории в 50 млн., телевизору — 13 лет, Интернет — 4 года, iPod — 3 года, в то время как Facebook добавил 200 миллионов пользователей менее чем за один год.

И, наконец, если бы Facebook был страной, то ее население было бы третьей в мире по величине, уступив только Китаю и Индии.

С каждым из этих потенциальных соединений мы выдумываем одну ссылку в цепи понимания — в конечном итоге укрепляя фундамент доверия жизненно важного значения по обмену идеями, общению, сотрудничеству и кооперации друг с другом. Тем не менее, несмотря на то, что прикладной характер социальных сетей очевиден, первоначальная трудность получения доступа к Facebook и другим социальным сетям через сеть правительства может быть обескураживающей и разочаровывающей. Мы должны делать это лучше. Мы должны быть подключенными более открыто. Использование социальных медиа является отличной идеей, которая растет в популярности, и может быть отличным инструментом для всех видов деятельности.

Размер аудитории может быть очень большим, а сообщения быстро распространяться. Мы должны иметь друзей в Facebook, иметь блоги и писать в твиттер. Нам нужны богатые каналы и подкасты с резюме сайтов (RSS), а также и LinkedIn. Эти и многие другие — это важные инструменты в создании ключевых и ценных стратегических связей для увеличения положительной корреляции между словами, делами и последствиями. Другим примером потенциала преимуществ и выгоды, связанных с подключением и расширением киберпространства можно найти в, пожалуй, одном из наименее вероятном для этого месте — Афганистане. В течение десятилетия или двух бумажные деньги больше не будут существовать, а электронные банковские и другие операции займут их место. Это будет способствовать дальнейшему подключению к нам способами, которые мы еще не начали ассимилировать в нашем обществе и наших культурных нормах — особенно в Соединенных Штатах. Как говорится, нужно следовать за деньгами. В процессе перестройки Афганистан может пропустить несетевые банковские операции, перейдя с бумажных денег прямо к операциям с мобильными телефонами и электронным вкладам. Подавляющее большинство афганских сил национальной безопасности в настоящее время получает зарплату электронными платежами и, после биометрической проверки, могут получить доступ к их деньгам через сотовые телефоны. Это уменьшает возможность для коррупции, исключая потоки бумажных денег и связанный с ним соблазн снять большие объемы

средств в процессе каждой передачи денег. Такой процесс позволяет афганцам использовать электронные носители по всей их стране.

Грозовые тучи на горизонте

Конечно, в то время как новые механизмы и технологии обеспечивают средства подключения и расширяют права и возможности следующего поколения, они также позволяют некоторым обеспечить свои каналы для распространения гнусных идеологий, для прозелитизма и участия в незаконной деятельности в этой значительной степени нерегулируемом виртуальном домене. Так как мы наблюдаем за погодой на горизонте киберморя, мы должны посмотреть на базовые технологии и их трансформационный эффект на нашу культуру, наши учреждения и нашу социальную ткань. Мы должны также выяснить, как все эти вещи связывают и взаимодействуют, чтобы умалить или усилить нашу коллективную безопасность. Каждый прилив приносит потенциальные проблемы в этой безопасности, что опасно игнорировать — кибер события могут охватывать весь диапазон от наблюдения на низшем уровне до DOS атак и разрушения инфраструктуры; от шпионажа и проникновений до реальных кинетических эффектов, от преступлений до войны. В любой день мы можем стать жертвой хакеров, кражи личных данных, а также «хактивистов». Наши системы бомбардируются ботнетами и вирусами. Троянские кони, черви, шпионские программы и спам продолжают существовать. Мы знаем, что эти угрозы реальны. Согласно профессионалам своего дела из Киберкомандования США, которое выполняет задачи Министерства обороны в области киберпространства, в среднем в день сети Пентагона подвергаются прощупыванию около 250000 раз в час; это внешняя разведка, пытающаяся взломать компьютеры США, и также террористы, ведущие активность на более 4000 веб-сайтах. В 2010 г. подрядчики Министерства обороны по киберзащите были атакованы, в результате чего более чем 24000 файлов и фрагментов данных было украдено.

Эти моря действительно штормит, и они так же неумолимы как в отношении отдельных людей, брошенных на произвол судьбы, так и предприятий, и даже национальных государств. Здесь, в Европе, этот вопрос имеет особый резонанс. В апреле 2007 г. три балтийские республики — Эстония, Латвия и Литва подвергались ряду DOS-атак, преимущественно пострадали серверы Эстонии и ее финансовая система. На следующий год Республика Грузия пережила не только кибератаку, но почти одновременное физическое нападение. Атаки сами по себе были вызывающими, хотя не являлись непреодолимыми. Что было труднее — так это приписать эти нападения и определить их происхождение. В то время как бомбы и ракеты, как правило, оставляют «отпечатки пальцев» и имеют обратный адрес, фотоны на волокнах сложно отслеживать. Как

заявил бывший заместитель министра обороны США Уильям Линн, «одно нажатие клавиши облетает дважды по всему миру в 300 миллисекунд, в то время как судебно-медицинская экспертиза, необходимая для идентификации злоумышленника, может занять несколько месяцев». Таким образом, не будучи в состоянии точно определить происхождение кибератаки для атрибуции, эта ситуация еще показывает и катастрофические последствия, которые могут быть достигнуты при объединении двух форм наступательной войны, укрепляя реальность киберпространства в качестве законной среды боевых действий. Эта атрибуция и усилия по судебному преследованию продолжают мешать, потому что в реальности нет согласованного определения того, что представляет собой кибератака и при этом в большинстве случаев нет физического результата нападения — воронок, затонувшего корабля или разрушения системы безопасности, в то время как целью являются, как правило, данные, последствия могут разниться от эксплуатации до деградации и разрушения, а поскольку данные не выглядят так же осязаемо, как некоторые другие, более традиционные типы целей, то и последствия могут выглядеть не так драматично. Долгосрочные эффекты, однако, могут быть более разрушительными и дорогостоящими, как в экономике, так и в человеческом капитале. Таким образом, потерпевшему от нападения оно является нападением, независимо от того, является это оружие бомбой или ботнетом. Аватары и иконки способствуют сохранению стерильной и неорганической среды, которая имеет тенденцию создать ложное чувство безопасности и отстраненности, но ранения, уничтожение и смерть могут быть вызваны довольно легко в эту эпоху «дот-боя». Конкретным примером этого может служить более быстрое и дальновидное использование киберпространства террористами. За последние 10 лет количество веб-сайтов, посвященных тому, что мы на Западе называем сайтами джихадистов-террористов, увеличилось в тысячу раз, и они используют свободу в Интернете в качестве форума для распространения своей пропаганды, привлечения средств и вербовки новообращенных. Джихадисты также используют Интернет как виртуальный класс, чтобы научить как делать бомбы и планировать нападения, в конечном счете, даже координируя и проведение атак через Интернет. В этом смысле для террористов Интернет стал недорогой сетью командования и управления по всему миру с неограниченным количеством узлов и отсутствием требований по обслуживанию или накладных расходов. Они имеют большой опыт по адаптированию широкого спектра инструментов для более полного использования отсутствия границ, политики, правил, а также анонимности в этом домене. Не сделайте ошибку — наши враги так же умны, как и хорошо финансируемы и, таким образом, инновации становятся улицей с двусторонним движением.

Балансировка открытого доступа и безопасности

Все это приводит к важному вопросу: как мы — индивидуально и коллективно — сбалансируем свободный и открытый доступ в такое виртуальное царство с необходимой защитой и правилами, обеспечив наш неизменный доступ к среде, которая является надежной, безопасной и способствует процветанию человечества в целом? Те же технологии, используемые обычными людьми для связи, сообщений и образования также используются теми, кто хочет вредить и разрушать. Существует напряженность в отношениях между этим желанием открытости и очень законным интересом по защите наших сетей и наших граждан. Будь то сдерживание угроз промышленного шпионажа, обеспечение избыточности системы в нашей интернет-зависимой инфраструктуре или улучшение судебных методов для проведения расследований и точного указания источника кибератаки, те, кто заинтересован в кибербезопасности, гонятся за теми же целями: максимальная защита конфиденциальной информации и одновременная возможность цельного соединения, функциональность и избыточность.

Найти правильный баланс, право установки на реостат, является ключевым фактором. Если мы хотим конкурировать на текущем рынке идей, если мы хотим, чтобы в полной мере пользоваться преимуществами достижений, таких как телемедицина, биометрия, отображение местности, виртуальное сотрудничество и невероятное множество разработанных и удобных для пользователей приложений, мы должны сделать это правильно. Мы должны защитить наши кибер сети в наших интересах, а не в ущерб нам. В вооруженных силах США сегодня мы боремся с этой дихотомией, даже на самом высоком уровне. Можно процитировать бывшего вице-председателя из Объединенного комитета начальников штабов генерала Джеймса Картрайта, сказавшего, что «мы не можем позволить командной цепи разорвать цепь информации». Для обеспечения непрерывного потока информации традиционные соединения (которые некоторые могут отнести к передовому опыту), которые препятствуют перекрестным потокам идей, должны быть разбиты. Нам необходимо разработать политику осмысленной, сконструировать и построить инновационные технологии, а в противном случае информировать об обсуждении для того, чтобы преодолеть пробелы «потребности — технология — политика». Мы видели позитивный потенциал этой среды в действии — будь то в джунглях Колумбии, на улицах Тегерана или на площади Тахир в центре Каира, а совсем недавно в Ливии и Сирии. В каждом случае активисты и технически подкованные сочувствующие объединили силы, используя подключение и потенциал кибердомена для получения результата, который Эрик Шмидт и Джаред Коэн чудесно охарактеризовали как ситуацию, когда «революция станет подкастом» с «политическими «флэш-мобами», о которых будут писать, отсылать твиты

и разрабатывать законопроект о правам человека для века Интернета». Как те, кто любит свободу слова, печати, вероисповедания, собраний и политического самоопределения, могут засвидетельствовать, поиск баланса между расширением прав и возможностей обездоленных без несправедливости может и будет трудным и непростым, и огромное количество пользователей — один миллиард, который растет, только усугубляет проблему.

Если мы собираемся успешно существовать в этом домене, нам нужно сделать так, чтобы вместе сочетать военный и гражданский, иностранный и отечественный, а также государственный и частный секторы. Каждая нация имеет свой собственный суверенитет, правоохранительные органы, подход к конфиденциальности, системы и нравы, а также сети и технологии. Однако в киберпространстве, возможно, больше, чем в любом другом домене, который мы привыкли эксплуатировать, коллективное целое действительно больше, чем сумма всех нас, работающих индивидуально. Как и в большинстве начинаний, слова имеют значение — таксономия важна. Таким образом, первый шаг — это согласование набора определений, формулирование круга полномочий, а также создание общей лексики. По большей части, это уже существует в военно-технологическом мире, но на самом деле это не выходит за рамки этого коллектива. Поскольку мы продолжаем бороться за установление физических границ киберпространства, мы должны определить что является и не является кибератакой. Это преступная деятельность? Шпионаж? Кибервойна? Враждебные намерения? Затем мы должны определить и согласовать, что следует предпринять, и что оправдано в каждой конкретной ситуации, на основе возможных, все еще неписаных законов, которые управляют действиями в этом диком море, как во времена войны, так и мира. Это, правда, очень милитаристские термины, однако, действия в этом домене во главе с военными будут проходить не часто, поэтому мы должны обеспечить наше межведомственное экспертное сообщество, а также профессионалов со стороны промышленности, которые связаны с этой дискуссией с самого начала. В НАТО они были. В результате на нашем жаргоне мы начали создавать то, что мы называем «правилами участия», правила, которые все 28 стран — членов альянса понимают, и на которые они согласны.

Киберакции НАТО

В середине ноября 2010 г. лидеры 28 государств — членов НАТО собрались в Лиссабоне на саммит. Одним из основных результатов этой успешной встречи стала новая стратегическая концепция НАТО, а одним из главных направлений этого основополагающего документа — как альянс смотрит в будущее — был кибердомен. Лиссабонский саммит постановил разработать или пересмотреть кибероборонную политику НАТО к середине лета, а также осуществить необхо-

димые сопровождающие действия и реализовать план. В июне 2011 г., выполняя задачи Лиссабона, политическая структура, ответственная за принятие решений в НАТО –Североатлантический Совет — принята новую политику НАТО по кибер обороне в сочетании с Планом действий. Работа с нашими союзниками и извлеченные уроки из таких событий, как кибератака в 2007 г. на Эстонию, привела к новой политике НАТО, сфокусированной на улучшении скоординированного многонационального подхода и укреплении наших коллективных и индивидуальных способностей по киберзащите для предотвращения угроз и улучшения наших ответов. В 2003 г. НАТО основала общий Центр по передовой киберзащите в столице Эстонии Таллинне. Он был аккредитован в качестве центра передового опыта НАТО в 2008 г. Это международная организация, которая занимается образованием, консультациями, научными исследованиями и разработкой в сфере кибербезопасности. Миссией центра является расширение возможностей, сотрудничество и обмен информацией между странами НАТО и партнерами по киберзащите. Кроме того, центр недавно установил важные и формальные отношения с Symantec Corporation для содействия сотрудничеству по исследованию Интернет угроз и контрмер. Сотрудничество между этими двумя организациями помогает этому центру в дальнейшем исследовать новые идеи, чтобы наилучшим образом понимать, оперировать и осуществлять навигацию в еще бесконтрольном и неуправляемом пространстве этого домена.

Мы также создали в НАТО структуру по реагированию на компьютерные инциденты (CIRC), которая получила мандат на высшем уровне по расширению возможностей и потенциала для выявления, оценки, предупреждения, защиты и восстановления от кибератак. Этот центр стал полностью готовым к работе в 2012 г., и это является важным шагом в расширении функции для поддержки кибер предупреждений и оценки ущерба как части единой структуры комплексного кризисного управления.

Кроме того, поскольку, как представляется все более очевидным, что кибер будет играть важную роль в любом будущем кризисе, нам нужно интегрировать систему кибер предупреждения в наше планирование и, возможно, разработать способы по оценки ущерба от кибератак, а также иметь возможность определять как кибератаки согласуются с использованием других инструментов власти (дипломатических, военных , экономических и др.) в условиях кризиса. Таким образом, мы создали ячейку по кибероборонe в рамках нашего нового кризисного центра управления операциями, который будет включать в себя возможности укрепления национальной и международной поддержки кибер знания в общей системе предупреждения, оценки и кризисного реагирования.

Если НАТО подвергается нападению, CIRC обеспечит техническую защиту и надлежащую реакцию, в сочетании с советом по киберуправлению, который единственный несет ответственность за координацию киберзащиты всего

Альянса через серию меморандумов о взаимопонимании между организацией по кибероборонe каждой страны и советом. Если индивидуальный союзник подвергается нападению, то все обстоит немного сложнее, особенно когда дело доходит до коллективной обороны. Понимание всего этого в контексте оригинального Вашингтонского соглашения, подписанного в ходе совсем другого времени в 1949 г., является первостепенным. Статья 5 договора НАТО, действительно, является сердцем соглашения — она гласит, что нападение на одного члена рассматривается нападением на всех. Статья 6 этого договора определяет, что является вооруженной атакой, сосредоточив внимание на географии, нападении на территорию, корабли в море, атаки на воздушные суда, войска и тому подобное. В 1949 г., однако, немногие, если таковые имеются, могли бы подумать об этом новом кибермире. В результате, в рамках НАТО в частности, мы должны определить, что такое нападение. Изменяется ли оно от одного члена Альянса к другому? Опять же, у каждой нации имеется свой собственный суверенитет, свои законы, свои правоохранительные органы и свой собственный подход к конфиденциальности и безопасности. Как союзники будут реагировать на кибер события существенной величины или какой набор мер союзники одобрят в ответ на кибератаку — это решения, которые должны сделать отдельные страны. Тем не менее, новая киберполитика НАТО довольно четко показывает, что любое решение по коллективному ответу (применение статьи 5) будет политическим, которое примут высокопоставленные политики из Альянса и стран-членов, а не военные или технические группы реагирования. Следует отметить, что единственный раз, когда НАТО сослалась на статью 5 — это было 12 сентября 2001 г., после террористических атак 9/11 на США.

Сотрудничество в более широком контексте

Этот новый и неоспоримый аспект военных действий, скорее всего, проявится больше как методология войны, которая продолжает развиваться. Нам нужно понять это новое кибер измерение ведения войны и как с ним бороться, мы должны вступить в схватку с понятием, что военное вмешательство в этой области является всего лишь небольшой частью головоломки. В Соединенных Штатах Министерству внутренней безопасности, очевидно, правильно отведена ведущая роль в этом стремлении. Минобороны является лишь одним членом команды, и мы во многом предназначены для поддержки членов другого межведомственного сообщества. Таким образом, мы должны продолжать пытаться понять кибербезопасность в большем межведомственном контексте, возможно, извлекая уроки из другого комплексного подхода, применяющегося для транснациональных и межведомственных вызовов, связанных с незаконным оборотом.

Нам удалось наладить и укрепить выдающееся межведомственное и международное сотрудничество в Объединенной межведомственной Целевой группе «Юг» в Ки-Уэст, штат Флорида, а также в аналогичной организации под названием Объединенный Межведомственный Центр по противодействию незаконному обороту, здесь, в Европе. Эти потенциальные модели, которые могут применяться в мире кибербезопасности, возможно, в форме совместной межведомственной целевой группы, в идеале включая правоохранительные органы международного права и другие элементы с ростом и развитием организации. Наконец, хотя правительство несет большую ответственность за обеспечение механизмов обеспечения наших интересов в киберпространстве, кибербезопасность, как говорят моряки, — это «все руки на палубе» эволюции. Хотя есть время от времени сильные перекрестные потоки между тем, что мы традиционно рассматриваем в роли национального органа и роли государственно-частных предприятий один на один с нашей всеобъемлющей безопасностью, мы должны привлечь опытных профессионалов в промышленности и в международных организациях. Лучшие практики уже распределены между многими экспертами по кибербезопасности в форумах по всему миру. Тем не менее, общий недостаток доверия между различными игроками (включая корпорации, правительственные структуры, и даже сами народы) исключает ускоренный роста наших возможностей по киберзащите. Нам нужно прекратить эти подозрения и работать вместе в направлении наших общих целей — это явно в наших общих жизненно важных национальных интересах.

Если корпорации инвестируют реальную энергию в обмен по развитию кибер возможностей, будь то в форме человеческого капитала, инвестиций или фактического аппаратного и программного обеспечения — нам необходимо обеспечить ясные стимулы. Какие преимущества существуют для промышленности, чтобы участвовать в этом процессе? Как будет такое сотрудничество и взаимодействие повышать их относительную конкурентоспособность, имидж и увеличивать их показатели? Мы обнаружили, что НАТО может играть ключевую роль в координации деятельности, а также создании правильных стимулов для участия. Одним из способов является подчеркивание участия таких компаний, путем внесения их в каталог доверенных фирм, способных предложить услуги по безопасности и соответствующие компоненты. Основным условием для включения в такой список будет приверженность и вклад в развивающийся обмен информацией. И есть другие способы. Кибер военные эксперты НАТО полагаются в большой степени на партнерскую форму через всех наших союзников, как в военной, так и в гражданской сфере. Все чаще мы находим, что нам необходимо развивать и использовать вклады со стороны частного сектора, так как промышленность будет абсолютно необходима, поскольку мы продвигаемся вперед. Это также то место,

где находится основная часть неограниченного инновационного мышления. Мы недавно провели конференцию в штаб-квартире НАТО при участии корпораций, ученых, военных, а также большого числа чиновников из многих стран, чтобы изучить эти связи между государственным и частным сектором, и как лучше интегрировать их в более крупный комплексный подход в области киберпространства. Многие замечательные выступления дали путь некоторым выдающимся инициативам, которые мы будем осуществлять в ближайшие недели и месяцы. Такие конференции будет регулярно проводиться, поскольку мы начинаем, чтобы закладывать основу для долгосрочного сотрудничества и кооперации.

Минобороны уже начало исследовать, как промышленность может помочь в этом отношении через государственно-частное партнерство, названное Несокрушимая Структура Безопасности. В соответствии с этим соглашением, исполнительный директор и главные офицеры по технологии основных информационных технологий (ИТ) в настоящее время периодически встречаются с высокопоставленными должностными лицами как в Минобороне и Министерстве внутренней безопасности, так и с директором Национальной разведки. В НАТО мы начали разговоры с целью рассмотрения создания похожей структуры, в которой ключевые европейские агентства, предприятия и правительства будут отобраны для участия в обмене информацией по кибербезопасности. Это информационное сотрудничество будет включать в себя все, начиная от угроз отказа до политических дебатов, исследований и инициатив в области развития. Эта последняя категория обеспечит потенциально большую отдачу от инвестиций, поскольку мы стремимся уровнять цикл оборонной промышленности и ИТ (который колеблется между 7 и 8 годами) и цикл технологического развития (что в среднем составляет от 1 до 2 лет — всего 24 месяца для разработки iPhone, например). Как выразился заместитель секретаря Линн, «это меньше времени, чем у нас есть для подготовки и защиты бюджета, а затем получения одобрения Конгресса, чем у [Apple] для получения iPhone. Это не приемлемый обмен».

Новое мышление

В контексте безопасности, развязывание мощностей киберморя изменило все, кроме нашего образа мышления. Мы просто не можем решать новые задачи, используя старые процессы мышления. Мы должны постоянно развиваться. И мы должны продолжить тестирование наших теорий и доктрин с объединенными, межведомственными и международными учениями и моделированиями. Агентство Перспективных Исследований Министерства обороны (DARPA) создает «макет Интернета», полигон по обучению моделирования, на котором мы смо-

жем проверить меры безопасности, ответы на атаки и как лучше интегрировать различные возможности и потенциал каждого игрока.

В 2010 году Министерство внутренней безопасности провело маневры по внутренней безопасности Cyber Storm 3. Они включали в себя федеральные и государственные структуры, частный сектор и международные организации, все работали вместе, чтобы оценить сильные и слабые стороны текущей политики, тактики, процедур и возможностей. Нам нужно продолжать проведение таких нелицеприятных оценок и тестов. Через них мы учимся, что не можем позволить себе ограничить наш собственный доступ к ценной информации, чтобы защитить себя от потенциально вредной деятельности. Скорее, мы должны быть технически подвижными и политически достаточно смелыми, чтобы опередить тех, кто стремится сделать вред в кибер-пространстве. Это маневренная война в кибер масштабе, и мы должны быть быстрыми. Кроме того, в сентябре 2011 г. Европейское командование США провело мероприятие под названием Combined Endeavor — учения по связи и компьютерным сетям, в которых приняли участие международные военные, тезничнеские и академические специалисты из 28 стран для того, чтобы сотрудничать и улучшить партнерские отношения с конечной целью укрепления коллективных возможностей киберзащиты. Темой маневров в этом году было «Информационное Доминирование Коалиции», а заседания были посвящены совершенствованию международной киберзащиты, практически осуществляя кибер информационный обмен, и институционализируя коалиционное киберобучение. Точно так же, в декабре НАТО провели свои основные ежегодные киберучения Cyber Coalition 2011. Более 100 специалистов приняли участие в учениях по кибер-обороне в штаб-квартирах НАТО в Брюсселе и Монсе, в том числе на национальных кибероборонных объектах в странах все собрались вместе, чтобы проверить технические и оперативные возможности Альянса по киберзащите. В обоих учениях были разработаны сценарии, требующие решения, координации и сотрудничества с техническими экспертами, политиками, а также органами управления. Оба были весьма успешными мероприятиями, и мы много узнали. Мы узнали, что мы сталкиваемся с общим вызовом и, таким образом, через открытое общение и сотрудничество, мы будем строить доверие между нашими странами. Самое главное, мы подчеркнули тот факт, что, хотя это невероятно сложная вещь для реализации, интернационализация кибербезопасности абсолютно возможна. Это также абсолютно необходимо.

Эта статья началась с аналогичной ссылки на киберморе. Как мы связаны в кибермире интересно сравнить с морской областью, особенно в контексте проблем, с которыми человечество сталкивается в результате действий неприрученных океанов. Человечество две или три тысячи лет училось работать на море, у нас постепенно создавалось международное морское право, система буев, глобальная навигационная сеть и карты по указанию пути. В целом, мы создали систему. И

в 1980-х гг. международное сообщество собралось на крупнейших переговорах в истории человечества и создало Конвенцию Организации Объединенных Наций о морском праве. Потребовалось целое десятилетие, чтобы вести переговоры. Документ в более чем 200 страниц, это чрезвычайно сложный канон, но за редким исключением, для 195 суверенных подписавшихся государств это руководство для действия в море.

Теперь подобное обязательство назрело и относительно киберморя. Мы плыли в этом пространстве всерьез в течение примерно 20 лет, и реально создавали волны последние 10 лет. Тем не менее, по большей части, мы до сих пор не имеем надежных буев, мы до сих пор не имеем навигационной сетки, и мы все еще плаваем без современных карт. Мы не можем даже сказать, что у нас есть основные нормы поведения, ограничиваясь несколько очень конкретными карательными законами за самые вопиющие акты. Что еще более важно, мы не имеем тысячелетия, чтобы понять это. Нам не хватает времени. Наш министр обороны недавно прокомментировал, что «существует сильная вероятность того, что следующий Перл-Харбор, с которым мы столкнемся, вполне может быть кибератакой». С каждой миллисекундой этот ширящийся посредник растет в уязвимости быстрее, чем он растет в полезности, а институциональные правила и политика ползут где-то сзади.

Нам нужно догнать и, в конечном итоге, выйти на гребень этой основной волны. Мы должны согласиться на конкретный круг терминов, таких как «атака» и «инцидент» и что составляет каждый из них. Мы должны согласиться на политические рецепты, которые диктуют пропорциональность ответа, преследуя нападающих сквозь национальные границы, будь это географическая или виртуальная сеть линий и что-то еще. В 2011 г. киберстратегии Белого дома и Пентагона прошли долгий путь к каждой из этих целей, так же как и новая киберполитика НАТО, но мы должны подтолкнуть эти усилия дальше.

И мы должны делать это совместно: внутри и между правительствами и их учреждениями, внутри и между государственным и частным секторами, во всех академических институтах, и в наших общих домах. Кибербезопасность требует сложных и скоординированных ответов, которые двигаются со скоростью мысли. Разнообразие способностей, возможностей, и ответы на любые кибер задачи должны рассматриваться как сила, а не слабость, но только если действия и инструменты могут быть использованы синергетически. Это может быть только в том случае, когда все заинтересованные стороны принимают общее видение безопасности, построенное на основе доверия и конфиденциальности, и достигается за счет координации, сотрудничества, и партнерства. Ни один из нас так не силен, как все из нас, работающие вместе.