ИНДЕКС КИБЕР-ГОТОВНОСТИ 2.0

ПЛАН КИБЕР-ГОТОВНОСТИ: ДОКЛАД И ИНДЕКС

Ведущий исследователь: Мелисса Хатауэй

Крис Демчак, Джейсон Кербен, Дженнифер МакАрдл, Франческа Спидальери

Ноябрь 2015

POTOMAC INSTITUTE FOR POLICY STUDIES

Опубликовано Потомакским Институтом политических исследований

Potomac Institute for Policy Studies
901 N.Stuart St, Suite 1200
Arlington, VA, 22203
www.potomacinstitute.org
Тел: +1(703) 525-0770; Факс: +1(703) 525-0299

E-почта: *CyberReadinessIndex2.0@potomacinstitute.org*

Следуйте за нами на Twitter:
@CyberReadyIndex

Благодарность

Потомакский Институт политических исследований хотел бы поблагодарить Отдел ИКТ Приложений и Кибербезопасности, Международного союза электросвязи, а также Межамериканский Комитет по борьбе с терроризмом при Организации американских государств за их постоянную поддержку. Авторы хотели бы также поблагодарить Шерри Лавлес и Алекса Талиесин за их редакторскую и оформительскую работу.

Перевод документа на Русский язык, а также его редактирование и публикация, были произведены при участии и поддержке Digital.Report Analytics (*https://digital.report*), информационно-аналитической группы экспертов специализирующихся на информационной и кибер-безопасности в Евразии, при канадском Фонде СекДев. Фонд СекДев, один из мировых лидеров по вопросам кибербезопасности, работает в пост-Советском киберпространстве с 1990х годов в тесном сотрудничестве с государственными, частными и общественными организациями продвигая безопасное использование ИКТ во всех сферах жизни.

ИНДЕКС КИБЕР-ГОТОВНОСТИ 2.0

ПЛАН КИБЕР-ГОТОВНОСТИ: ДОКЛАД И ИНДЕКС

СОДЕРЖАНИЕ

ИНДЕКС КИБЕР-ГОТОВНОСТИ 2.0

ПЛАН КИБЕР-ГОТОВНОСТИ: ДОКЛАД И ИНДЕКС

Ведущий исследователь: Мелисса Хатауэй
Крис Демчак, Джейсон Кербен,
Дженнифер МакАрдл, Франческа Спидальери

Индекс кибер-готовности 2.0 основан на содержании Индекса кибер-готовности 1.0, опубликованного в ноябре 2013 г.

ВВЕДЕНИЕ

На сегодняшний день ни одна из стран не находится в состоянии кибер-готовности

Является общепризнанным фактом, что глобальный экономический рост зависит от скорейшего внедрения в жизнь новых информационно-коммуникационных технологий (ИКТ) и обеспечения доступа общества в Интернету. Именно поэтому, планы развития цифровых технологий каждого государства содержат обещания стимулировать экономический рост, повышать эффективность услуг, их качество и доступность, содействовать инновациям и росту производительности, а также обеспечивать разумное управление в этой сфере. Однако доступность, взаимосвязанность и гибкость глобальной коммуникационной инфраструктуры таят в себе и уязвимость. Объемы, количество, скорость возникновения и сложность угроз нашим сетевым системам и инфраструктурам весьма реальны и постоянно растут. Взлом баз данных, криминальная деятельность, прерывание обслуживания в результате действий злоумышленников, а также уничтожение собственности становятся слишком обыденными явлениями и угрожают росту интернет-экономики.

Мировые лидеры осознают, что растущее проникновение интернета ведет к экономическому росту только тогда, когда базовые элементы инфраструктуры и связанные с ней устройства безопасны для пользователей и сети. Поэтому страны вынуждены согласовывать видение будущего развития своих экономик с приоритетами национальной безопасности.

До настоящего времени не существовало всеобъемлющей, сравнительной и экспериментальной методологии, которая позволила бы

оценить способности и приверженность стран в деле обеспечения безопасности своих национальных кибер-структур и цифровых услуг, от которых зависит их информационное будущее и развитие. Индекс кибер-готовности (ИКГ)[1] 1.0 представил новый взгляд на изучение этой проблематики, и создавался с целью инициирования международной дискуссии и стимуляции международной деятельности для решения экономических проблем, связанных с угрозами безопасности в киберпространстве.

На основе подходов и методов ИКГ 1.0, настоящий Индекс кибер-готовности 2.0 рассматривает ситуацию в 125 странах, в которых применяются и используются, либо планируются к применению и использованию, ИКТ и интернет, а также применяет объективную методологию для оценки готовности и приверженности каждой из стран к обеспечению кибербезопасности в семи (7) ключевых категориях. Применяя эту методологию, любая страна может яснее представить проблемы, с которыми она столкнется в своей интернет-инфраструктуре, а также следующие из этих проблем зависимости и уязвимости[2]. В частности, в ИКГ 2.0 производится оценка уровня готовности стран к определенному виду кибер-угроз, а также определяются области, где руководители государств могли бы улучшить или исправить положение дел в стране посредством усиления или исправления законодательных норм, политик, стандартов, рыночных рычагов (т.е. постановлений и стимулов), а также предпринять другие инициативы для обеспечения информационной безопасности и защиты экономических интересов страны.

ОБОСНОВАНИЕ

В большинстве стран приняты экономические стратегии основанные на ИКТ решениях, а также ведется работа направленная на обеспечение надежных и доступных средств коммуникации для каждого домохозяйства и бизнеса для того, чтобы привести свою страну и информационное сообщество в цифровую эпоху[3]. Такие инициативы экономической модернизации, как интернет-правительство (e-government), интернет-банкинг, интернет-здравоохранение, интернет-образование, следующие поколения энергосетей, автоматизированные элементы транспортной инфраструктуры и другие общественно-важные услуги, возглавляют экономические повестки дня многих стран. Например, китайская стратегия Интернет Плюс декларирует своими целями активное стимулирование развития интернет-коммерции, промышленных информационных сетей и интернет-банкинга, а также способствование росту новых производств наряду с активным развитием присутствия национальных компаний в интернете[4]. Как и многие другие страны, Китай видит в интернете ключевой фактор дальнейшего роста и широкие возможности для развития. Премьер-министр Индии, г-н Моди, также высказал свое намерение трансформировать свою страну в «экономику знаний, оснащенную цифровыми технологиями», используя всемирно признанные компетенции страны в области информационных технологий (ИТ) для создания рабочих мест в ИТ, телекоммуникациях, а также на рынках электронных устройств. Более того, Индия стремится стать лидером инноваций в области ИКТ-решений для здра-

Страны должны согласовать видение будущего развития своих экономик с приоритетами национальной безопасности

воохранения, управления знаниями и образованием, а также на финансовых рынках[5]. Наконец, Европейская Комиссия работает над созданием действенного единого рынка цифровых услуг, который бы обеспечил свободное перемещение товаров, услуг, капитала и бизнесов. Успешная реализация «Стратегии единого рынка цифровых услуг» по оценкам специалистов приведет к увеличению ВВП Евросоюза на 415 миллиардов Евро в год[6].

Правительства, в особенности развивающихся стран, принимают еще более агрессивные стратегии в области применения и развития ИКТ для того, чтобы предоставить дополнительные услуги миллионам своих граждан, тем самым еще более создавая и развивая сопутствующие экономические выгоды[7]. По оценкам Всемирного банка, каждые дополнительные 10% населения, получающие доступ в интернет, приводят к росту ВВП на 1-2%[8]. Более того, последние исследования демонстрируют, что правительства и деловые круги все более четко осознают, что использование интернета и развитие ИКТ повысит их долгосрочную конкурентоспособность и уровень благосостояния общества, потенциально привнося до 8% к национальному ВВП[9]. Некоторые исследовательские отчеты идут дальше, предполагая, что модернизация промышленных систем (т.е. энергосетей, нефте- и газопроводов, производственных линий и т.п.) составляет 46% объема современной глобальной экономики и в течение последующих десяти лет потенциально может вырасти до 50%[10].

Страны не могут себе позволить игнорировать такие экономические возможности. Но лишь немногие принимают в расчет такие факторы, как возможная уязвимость критически важных услуг, нарушение тайны личной жизни и приватности граждан, кража коммерческих и государственных секретов, а также последствия интернет-мошенничества и киберпреступлений. Все это может вести к ущербу национальной и экономической безопасности. Если говорить более простыми словами: кибер-небезопасность – это налог на экономический рост[11].

Кибер-небезопасность – это налог на экономический рост.

К примеру, по некоторым оценкам, экономики стран Большой двадцатки (G20) потеряли в общей сложности 2,5 миллиона рабочих мест из-за распространения контрафактной и пиратской продукции, а Правительства и потребители теряют из-за кибер-преступников до 125 миллиардов долларов США налоговых поступлений в год[12]. США оценивают ущерб своей экономике от краж интеллектуальной собственности (ИС) в 300 миллиардов долларов ежегодно. Это соответствует 1% ВВП страны[13]. Другие исследования, проводившиеся в Нидерландах, Великобритании и Германии дают схожие по уровню оценки потери ВВП этих стран. Ни одна страна не может позволить себе терять даже 1% ВВП в результате противоправной кибер-деятельности третьих лиц. Со все большим проникновением интернета и развитием ИКТ подверженность такому урону, сопутствующие риски, и экономический ущерб будут расти экспонентно, если безопасность и устойчивость системы не будут заложены в саму основу стратегий проводимой модернизации.

Осознание подобного ущерба экономике заставит руководства стран более тщательно согласовывать свои планы в области развития эко-

Устойчивые и взаимосвязанные сообщества должны обеспечивать модернизацию с учетом норм безопасности.

номики и безопасности, инвестируя в будущие выгоды развития в рамках обоих приоритетов[14]. Обеспечивая прозрачность информации об экономическом ущербе, создаваемом низким уровнем безопасности, может подстегнуть интерес к снижению таких убытков на глобальном и национальных уровнях. ИКГ 2.0 содержит рамочный подход, который позволит странам обеспечить экономический рост устойчивого, коммуникационного и информационного общества с учетом норм безопасности.

ИНДЕКС КИБЕР-ГОТОВНОСТИ 2.0: МЕТОДОЛОГИЯ

Индекс кибер-готовности 2.0 включает в себя две основных составляющих:

1) Во-первых, он предназначен для того, чтобы предоставить главам государств и правительств информацию о том, какие шаги они могли бы предпринять для повышения уровня защиты их стран, которые становятся все более взаимосвязанными с окружающим миром, а также для обеспечения дальнейшего роста ВВП. Такая информация становится доступной на основе оценки степени готовности и приверженности страны вопросам безопасности и устойчивости.

2) Во-вторых, ИКГ определяет термин «кибер-готовность» страны, а также предлагает основные компоненты кибер-готовности с тем, чтобы

Недостаточно сведений: сведения недостаточны, либо их предстоит еще найти. Возможно, что данные существуют, но их нет в открытом доступе, либо они засекречены.

Частично действующий: Имеются свидетельства наличия документов, деятельности и/или финансирования. Однако такие документы и/или действия могут быть неполными, несовершенными, либо находиться на ранних стадиях реализации. Несмотря на их наличие, степень совершенства инициатив определить сложно.

Полностью действующий: сведения позволяют классифицировать деятельность как зрелую, функциональную и результативную[15].

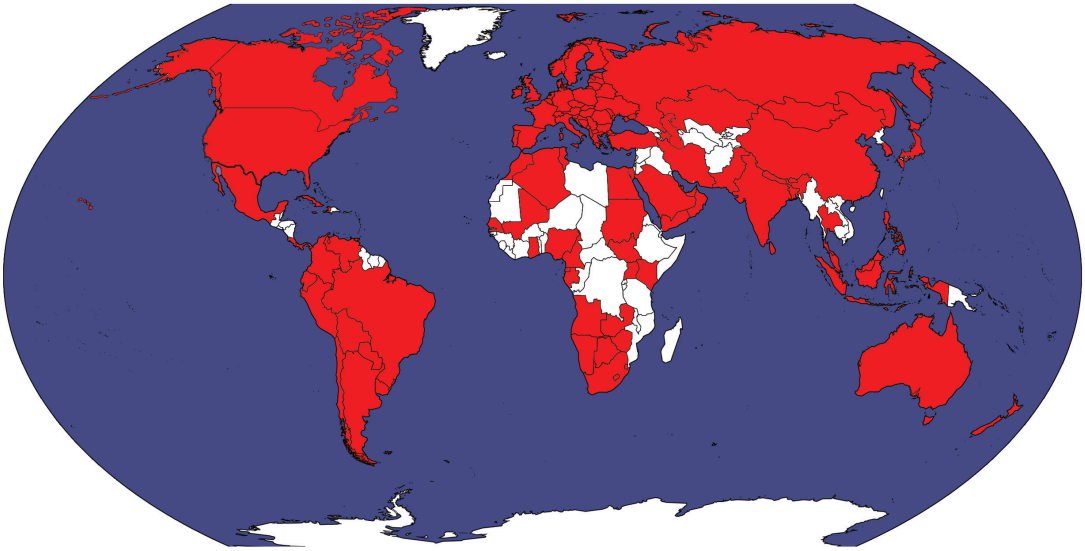

Рис. 1. Страны, представленные в ИКГ 2.0

Алжир	Колумбия	Израиль	Нидерланды	Шри Ланка
Андорра	Коста-Рика	Италия	Новая Зеландия	Сент-Киттс и Невис
Ангола	Хорватия	Япония	Нигерия	Сент-Винсент
Антигуа и Барбуда	Куба	Казахстан	Норвегия	Судан
Армения	Кипр	Кения	Оман	Свазиленд
Аргентина	Чехия	Кыргызстан	Пакистан	Швеция
Австралия	Дания	Латвия	Парагвай	Швейцария
Австрия	Джибути	Ливан	Панама	Тайвань
Азербайджан	Эквадор	Лесото	Перу	Македония
Бахрейн	Египет	Литва	Филиппины	Таиланд
Бангладеш	Эстония	Люксембург	Польша	Тринидад и Тобаго
Барбадос	Финляндия	Макао (Китай)	Португалия	Тунис
Беларусь	Франция	Малайзия	Катар	Турция
Бельгия	Габон	Мальдивы	Румыния	Уганда
Бутан	Гамбия	Мали	Россия	Украина
Боливия	Германия	Мальта	Саудовская Аравия	ОАЕ
Босния и Герцоговина	Гана	Маврикий	Сенегал	Великобритания
Ботсвана	Греция	Мексика	Сербия	США
Бразилия	Гонконг	Молдова	Сейшелы	Уругвай
Бруней	Венгрия	Монголия	Сингапур	Узбекистан
Болгария	Исландия	Монако	Словакия	Венесуэла
Камерун	Индия	Черногория	Словения	Вьетнам
Канада	Индонезия	Марокко	ЮАР	Йемен
Чили	Иран	Намибия	Южная Корея	Замбия
Китай	Ирландия	Непал	Испания	Зимбабве

Табл. 1. Страны, представленные в ИКГ 2.0 (в порядке, соответствующем латинскому алфавиту)

страны и правительства могли ориентироваться на определенные параметры.

Методология ИКГ 2.0 представляет собой уникальный, полезный и удобный в использовании инструмент для оценки глубины разрыва между нынешним положением дел с кибер-безопасностью в стране и кибер-возможностями в этой сфере, которые необходимы для достижения запланированного экономического развития. Основная матрица, разработанная и использовавшаяся в этом анализе, включает более 70 уникальных индикаторов в рамках следующих семи элементов:

1. Национальная стратегия;
2. Реагирование на инциденты;
3. Интернет-преступность и правоохранительная практика;
4. Обмен информацией;
5. Инвестиции в исследования и разработки (ИР);
6. Дипломатия и торговля;
7. Оборона и реакция на кризисные ситуации.

Оценка каждой страны основывается на данных, взятых из заслуживающих доверия первичных источников, а каждая уникальная информация приводится на основе результатов проведенных эмпирических исследований и документации. Страны оцениваются по всем индикаторам по трехбалльной шкале кибер-готовности: недостаточно сведений, частично действующий, полностью действующий.

Методология ИКГ 2.0 используется для оценки кибер-готовности 125 стран, включая оценки готовности и приверженности стран в вопросах кибер-безопасности, и устойчивость инфраструктур и жизненно-важных услуг (Рисунок 1 и Таблица 1).

В список стран, проанализированных ИКГ, включены 75 государств занимающих верхние позиции в *Индексе развития* ИКТ (ИРИ) Международного союза электросвязи (МСЭ), т.е. страны с более высоким развитием интернета. Страны-члены G20 были включены по причине того, что они создают 90% глобального ВВП, 80% международной торговли, в них живет 64% населения планеты, а также в этих странах выбрасывается в атмосферу 84% загрязнений от ископаемых видов топлива.

Для обеспечения региональной репрезентативности, остальные страны отбирались из стран членов: Организации экономического сотрудничества и развития (ОЭСР), Африканского экономического сообщества (АЭС), Латиноамериканской ассоциации интеграции (ЛАИ), Азиатско-Тихоокеанского экономического сотрудничества (АТЭС), Центрально-Азиатского регионального экономического сотрудничества (ЦАРЭС), Совета сотрудничества арабских государств Персидского залива (ССАГПЗ), Ассоциации регионального сотрудничества Южной Азии (СААРК), и Североамериканского соглашения о зоне свободной торговли. Страны, входящие в эти региональные экономические союзы, часто включаются в ИРИ, а также в Индекс сетевой готовности (ИСГ) Всемирного экономического форума (ВЭФ). Такой подход обеспечивает уверенность в том, что каждая из стран, рассматриваемая в отчете, развивает ИКТ. А также, активно инвестирует в доступные и широко распространенные интернет-услуги с целью стимуляции экономического роста.

Учитывая, что ССАГПЗ не представляет весь Ближний Восток, в настоящий индекс были вклю-

чены три страны этого региона с наиболее высоким ВВП, и не входящие в ССАГПЗ: Иран, Йемен и Ливан[16].

Обзор полученных 125 стран представляет значительную часть всей планеты и демонстрирует все имеющиеся глобальные различия, а также представительность отбора списка стран для ИКГ 2.0.

ИКГ 2.0 концентрируется на взаимозависимости между экономикой и безопасностью (или ее недостаточным уровнем), что позволяет каждой стране оценить свою готовность к возможным вызовам в киберпространстве, а также создает базу для формирования политик и стратегий, оперативных и институциональных инициатив, планирования ресурсов, создания законов и подзаконных актов, а также формирования и использования других рычагов рыночного влияния. Использование ИКГ 2.0 повысит осведомленность о взаимосвязи между устойчивым развитием киберпространства и ростом ВВП в любой стране, особенно с учетом того, что будущее экономики и ВВП любой страны непременно связано с технологиями и развитием интернета и услуг в нем. Кроме того, ИКГ дает основу для понимания глубины ущерба, наносимого экономикам кибер-преступниками, а также важность вопросов цифровой национальной безопасности в планах развития экономики и ИКТ. Эта методология может оказать помощь в принятии логически обоснованных решений в области реагирования и предотвращения потенциальных проблем в области безопасности.

Наконец, ИКГ 2.0 предоставляет международным организациям, таким как МСЭ, ВЭФ, Организация американских государств (ОАГ), Межамериканский банк развития (МБР), Всемирный банк и многие другие, рамочный подход для реализации их инициатив в этой области, а также основу для экспертных международных дискуссий.

Детальное описание семи основных категорий методологии ИКГ 2.0 приводится ниже. Каждый раздел посвящен одной категории и как минимум десяти индикаторам, с помощью которых оценивается кибер-готовность государств. Кроме того, приводятся примеры конкретных стран для демонстрации инновационных и мультикультурных решений повышения кибер-готовности государств. Такие примеры ни в коем случае не следует рассматривать как пример для подражания, однако они отражают различные подходы на государственном уровне.

1. НАЦИОНАЛЬНАЯ СТРАТЕГИЯ

Первая, и наиболее важная, категория, по которой определяется кибер-готовность страны, - это наличие разработанной и опубликованной Национальной стратегии кибербезопасности, в которой согласованы видение будущего экономического развития страны с положениями ее национальной безопасности. Интернет, широкополосные сети, мобильные приложения, кибер-услуги, программное обеспечение и вычислительное оборудование являются основой цифровых национальных экономик и информационно-коммуникационного будущего стран[17]. Интернет и ИКТ стали основой для социальных платформ (таких как Facebook™, Twitter™, Instagram™, Renren™, VKontakte™, и др.), бизнес-платформ, критически важных для функционирования общества услуг и инфраструктур, а также для глобальной экономики в целом[18]. Взаимозависимость и взаимная информационная связь стали характерны для всех секторов экономики. Так, современные производства используют системы промышленного контроля

и робототехнику для повышения производительности, и снижения зависимости от ручного труда. Современное сельское хозяйство использует интернет-устройства (Internet Protocols) для определения сроков и необходимости использования удобрений и регулирования сроков полива угодий. Интернет-устройства также размещаются на скоте, для определения мест пастбищ и водопоя, а также постоянного мониторинга состояния здоровья животных. Электронная торговля, свободное трансграничное перемещение товаров и услуг постепенно занимают место старых витрин и складов, позволяя доставлять товары прямо к дверям жилищ или базам оптовой торговли вскоре после размещения онлайн-заказа. Системы транспортировки в настоящее время широко используют сенсоры, мобильные устройства, а также автоматические терминалы для управления пассажиро- и грузопотоками, а также для продажи и доставки билетов. Оснащенные электронными системами города используют геолокационные устройства для определения скорости и положения в пространстве транспортных средств, а также выявления и предотвращения нарушений ПДД. Инновации в сфере здравоохранения позволяют оцифровать записи поликлиник и больниц, а также позволяют применять облачные технологии для доступа к информации о здоровье граждан в любой точке мира, чтобы обеспечить им качественное лечение. Телемедицина использует высокоскоростной доступ в интернет для дистанционного предоставления услуг и консультаций в районы с недостатком медперсонала. И, наконец, финансовые ИТ-системы ежедневно совершают обмен и перевод валют на суммы в триллионы долларов, на рынках ресурсов ведется торговля с использованием цифровых валют, а интернет-банкинг постепенно заменяет многие услуги обычных, физических отделений банков.

При этом, угрозы сетевым информационным структурам постоянно растут и развиваются. Страны начинают осознавать серьезность этих угроз и документировать необходимость защиты инфраструктур, данных, страны в целом, а также многих других уязвимых точек. Всесторонняя национальная стратегия кибербезопасности должна в экономических терминах описывать угрозы для страны, а также содержать необходимые шаги, программы и инициативы, которые следует предпринять и реализовать для нивелирования этих угроз и защиты систем коммуникаций и ИКТ, которые используются гражданами, бизнесом и правительственными учреждениями[19]. Стратегия также должна содержать план развития интернета и ИКТ, а также включать такие инициативы, которые поспособствуют минимизации потерь ВВП от кибер-угроз, а также повысят безопасность и устойчивость всей страны по отношению к ним.

Национальные стратегии кибербезопасности должны отражать экономическую важность кибербезопасности.

Действенная национальная стратегия кибербезопасности должна быть не просто написана и озвучена. Она должна быть принципиально реализуема. В настоящее время большинство тем, на которых концентрируются создатели этих стратегий, включают: определение организационной и институциональной ответственности в Правительстве; стимулирование осведомленности и роста образованности населения; создание систем и структур кризисного реаги-

рования и управления; расширение возможностей и полномочий правоохранительных органов для создания потенциала борьбы с киберпреступностью; создание и развитие государственно-частных партнерств и развитие надежных систем обмена информацией; направление ресурсов в исследования и инновации. Многие стратегии начинаются со статистических данных, дающих представление об уровне кибер-инцидентов и степени угрозы инфраструктурам, а также с перечисления существующих идентифицированных угроз. Эти данные используются для обоснования предлагаемого распределения ответственностей, а также роста финансирования определенных операций и организаций. Однако, такие стратегии редко содержат список приоритизирующий риски для определенных инфраструктур и услуг, и практически никогда не проводят оценку соизмеримости рисков с выделением требуемых ресурсов для их минимизации и предотвращения убытков. Действенная национальная стратегия кибербезопасности должна описывать существующую проблему или проблемы в экономических терминах; определять и наделять полномочиями компетентные органы[20], которые будут нести ответственность за реализацию стратегии; содержать четкие, измеримые, достижимые, проверяемые и ограниченные по времени цели в рабочем плане; а также осмыслить и признать необходимость выделения ограниченных ресурсов (таких как политическая воля, финансы, время и человеческие ресурсы) для достижения ожидаемых уровней безопасности и экономического роста.

Как минимум, около 67 стран уже опубликовали свои стратегии кибербезопасности (во многих других они находятся в стадии разработки), определяя ключевые шаги, которые призваны повысить уровень национальной безопасности и системную устойчивость по отношению к угрозам[21]. Во многих странах разработаны национальные стратегии безопасности (посвященные не только кибер-вопросам), которые координируют и направляют усилия правительств и по отношению к киберпространству. К сожалению, совсем немногие страны тесно увязывают свои национальную и экономическую безопасности, а тем более экономические измерения кибербезопасности. Еще меньшее число стран создают действительно реализуемые стратегии. Таким образом, практически каждая из стран имеет возможность пересмотреть и развить свою стратегию безопасности с тем, чтобы она реально отражала экономическое измерение кибербезопасности.

Среди основных элементов всесторонней национальной стратегии кибербезопасности должны присутствовать:

Заявление:

A. Публикация национальной стратегии кибербезопасности, которая содержит описание экономических возможностей и рисков, связанных с развитием ИКТ;

Организационные вопросы:

A. Определение компетентного органа и четкое определение его функций и полномочий;

B. Определение ключевых правительственных структур, связанных с реализацией, либо ответственных за реализацию стратегии кибербезопасности;

C. Определение ключевых бизнес-структур, связанных с реализацией, либо ответствен-

ных за реализацию стратегии кибербезопасности (признание взаимозависимости и ответственности бизнес-сектора);

Ресурсы:

A. Определение финансовых и человеческих ресурсов, требуемых и выделяемых для реализации стратегии;

B. Определение доли роста или снижения ВВП (гросс), ожидаемого в результате реализации/не реализации стратегии;

Реализация:

A. Определение механизмов, призванных обеспечить безопасность ключевых инфраструктур и развитие ИКТ;

B. Определение критических сервисов (не инфраструктур), которые в результате реализации стратегии получат более высокий уровень безопасности и устойчивости; и

C. Определение национальных стандартов по предоставлению непрерывных услуг (24 часа, 7 дней в неделю), а также требования к информированию о случаях недоступности любого из критически важных сервисов, производства или инфраструктуры.

Результаты полученные в рамках этой категории, равно как и в других шести, являются своего рода моментальным снимком динамичной и меняющейся ситуации. По ходу совершенствования и развития национальных стратегии кибербезопасности, дополнения в рамках этой категории будут отражать такие изменения. Существенные и значительные изменения будут тщательно отслеживаться и оцениваться. Таким образом, ИКГ 2.0 будет в режиме реального времени предоставлять самые свежие примеры для иллюстрации практических рекомендаций с тем, чтобы все страны могли успешно формулировать или пересматривать свои стратегии.

2. СИСТЕМЫ РЕАГИРОВАНИЯ

Второй категорией, определяющей уровень кибер-готовности страны, является наличие и поддержание на действующем уровне систем национального реагирования на инциденты. Зачастую, такие системы существуют в виде одной или более национальной Команды реагирования на угрозы кибербезопасности (Национальная КРКБ), либо Команда компьютерного реагирования (ККР), которые далее по тексту мы будем называть КРКБ, и которые несут ответственность за кризисное управление в случае чрезвычайных ИКТ-происшествий, вызванных техническими или природными явлениями, или действиями человека, и которые несут угрозу устойчивости критических сервисов и целостности инфраструктур[22]. К настоящему времени созданы и действуют 102 национальных КРКБ, а еще четыре находятся в стадии создания[23]. В состав КРКБ обычно входят ИТ-специалисты и практики-исследователи, представители частного сектора и госорганизаций. Помимо того, что КРКБ оперативно реагируют и устраняют кризисы в сфере высоких технологий, они также призваны упрочить возможности Правительств в области понимания характера и умения преодолевать кибер-угрозы. Таким образом, создание национального КРКБ является одним из основных элементов стратегии страны в области обеспечения безопасности и постоянного функционирования критических сервисов и инфраструктур, являющихся жизненно важными для обеспечения национальной безопасности и экономического роста[24].

Национальные КРКБ, в отличие от исключительно государственных органов, служат гораздо более широкому кругу бенефициаров: от Правительства до бизнесов, НПО и простых граждан. Действующий и реально работающий КРКБ в первую очередь призван обеспечить адекватный ответ на угрозы – т.е. иметь возможность немедленно реагировать на инциденты, купируя и минимизируя последствия в ходе развития кризиса[25]. Хотя формы организации КРКБ могут отличаться от случая к случаю, с учетом того, что ресурсы и возможности стран не равны, эти специализированные организации должны в любом случае быть способны осуществлять ряд предупреждающих и ответных функций, а также осуществлять превентивную, образовательную деятельность, одновременно реализуя управленческие функции в области обеспечения качества систем и услуг безопасности. Такие функции и деятельности должны включать, но не ограничиваться: обеспечение общественного согласия и общего понимания угроз, с которыми может столкнуться страна; публикация предупреждений и оповещений о кибер-уязвимостях и угрозах; поддержка осведомленности в вопросах кибербезопасности; определение, купирование, минимизация и устранение кибер-угроз с предоставлением информации об извлеченных уроках (для общественного обсуждения и информирования); координация работ во время инцидентов; а также поддержка реализации национальной стратегии кибербезопасности.

Так, например, национальная КРКБ Сингапура (SingCERT) создавалась в 1997 году силами Департамента по развитию информации и коммуникаций Сингапура (Infocomm Development Authority of Singapore, IDA) при сотрудничестве с Национальным университетом Сингапура (НУС). Впоследствии, группа стала составной частью Агентства кибербезопасности (АКБ) Сингапура. SingCERT создавалась как единый центр реагирования на ИТ-угрозы и кризисы: орган определения, предотвращения и разрешения инцидентов в области компьютерной и интернет-безопасности. SingCERT предоставляет техническую помощь и координирует деятельность в области преодоления и реагирования на кибер-угрозы, определяет потенциальные кибер-преступления и предотвращает их, своевременно распространяет информацию о возникающих угрозах, а также координирует свою деятельность с деятельностью других агентств в области обеспечения информационной безопасности[26]. SingCERT также организовывал и проводил учения по компьютерной безопасности в рамках Ассоциации стран Юго-Восточной Азии (АСЕАН) и Компьютерной группы реагирования на чрезвычайные ситуации Азиатско-Тихоокеанского региона (APCERT). Кроме того, Сингапур является страной, в которой функционируют семь членов Форума компьютерных групп реагирования и безопасности (FIRST).

Потенциал Бразилии состоит из национальной команды реагирования на чрезвычайные ситуации, CERT.BR, а также тридцати региональных КРКБ, работающих в четырех штатах страны и осуществляющих свою деятельность под руководством Бразильского наблюдательного комитета по интернету. Этот комитет является негосударственной организацией с широким представительством, и основным органом, ответственным за сетевую безопасность и реагирование на чрезвычайные ситуации в ИКТ в Бразилии[27]. Бразильский CERT.BR несет ответственность за непосредственное реагирование на кризисные ситуации, рост осведомленности граждан в вопросах сетевой безопасности, сбор данных о кибер-угрозах и возможных взломах и проникновениях, а также за координацию действий с многочисленными заинтересованными

сторонами, включая другие КРКБ, исследовательские организации, организации частного сектора. Кроме прочего, надо отметить, что в состав бразильских КРКБ входят представители финансового сектора, армии, Правительства и университетов страны[28].

Постоянство и надежность критических сервисов являются залогом национальной безопасности и экономического роста.

Помимо национальных КРКБ, созданы и существуют также и региональные организации подобного рода, которые призваны координировать и обеспечивать эффективность реакции на кризисные ситуации в своих регионах. Так, AfricaCERT является некоммерческой организацией, которая объединяет 11 стран Африки и является форумом по сотрудничеству и обмену технической информацией между операторами интернет-сетей в странах региона. Среди основных целей AfricaCERT: координация действий КРКБ стран Африки в преодолении кризисных ситуаций; помощь в организации КРКБ в странах, которые обладают невысоким потенциалом в области обеспечения безопасности; организация и поддержка в области предотвращения инцидентов и кризисов, а также организация образовательных программ в области ИКТ-безопасности; облегчение обмена информацией; а также внедрение и реализация лучшего опыта в области обеспечения кибер-безопасности. Подобным же образом, APCERT (региональный азиатско-тихоокеанский КРКБ) объединяет 28 КРКБ стран-членов и других экспертов по безопасности в регионе, и ставит своей целью повышение осведомленности и уровня экспертизы в деле предотвращения и преодоления инцидентов в области компьютерной безопасности в регионе[29]. Миссия APCERT – создание «чистого, безопасного и надежного» киберпространства посредством развития глобального сотрудничества. Для того, чтобы наладить эффективную коммуникацию по вопросам кибербезопасности и кибер-угроз, организационная структура APCERT использует систему «контактных точек» (point-of-contact, POC), при которой каждая страна-член организации делегирует своего представителя, который является POC в случае кризисной ситуации. Делается это для того, чтобы ускорить коммуникации и сократить время реакции на инцидент[30]. Таким же образом Организация исламского сотрудничества компьютерных групп реагирования на чрезвычайные ситуации (OIC-CERT), в которую входят государства Ближнего Востока, Юго-Восточной Азии, Южной Азии, Африки и Центральной Азии – также активно действует в области сотрудничества между национальными КРКБ и самой OIC-CERT.

Помимо развития потенциала реагирования на угрозы и инциденты, страны также принимают участие в учениях по предотвращению кибер-угроз и реагированию на кризисы. Эти учения помогают странам получить опыт и развить навыки своих специалистов в области эффективного преодоления кризиса, а также повысить стрессовую и кризисную устойчивость национальных КРКБ. Так, в ноябре 2011 года Федеральное правительство Германии провело однодневные учения по планированию и реагиро-

ванию на кризисные ситуации. Целью этих учений было спланировать и создать процедуры реагирования правительственных органов на потенциальные многоцелевые атаки, которые могли бы включать: отказ в обслуживании (DDoS-атака) в отношении критически важных инфраструктур; внедрение вирусного ПО в банковские сети, вызывающего отказ банкоматов и блокировку пластиковых карт; а также создание ложного трафика в системах контроля воздушных перевозок[31]. Шведские Агентство по чрезвычайным ситуациям (MSB), Агентство почт и телеграфа (PTS) и Радио Служба национальной обороны (FRA) также проводят регулярные совместные курсы Старших офицеров информационной безопасности (CIAO) для соответствующих учреждений. Каждый из этих курсов завершается финальным учением – симуляцией крупного информационного кризиса, который затрагивает государственные органы и ключевых игроков рынка, причем в учениях принимают участие члены Парламента и старшие менеджеры (CEO) компаний, несущих ответственность за функционирование критически важных сервисов в Швеции. Эти учения позволяют выявить проблемы в области реализуемой кибер-политики и недостатки действующего законодательства, одновременно повышая образовательный уровень и опыт участников в области кибербезопасности[32]. Чехия в октябре 2015 года провела учения по реагированию на кризисные ситуации, которые фокусировались на преодолении угроз критически важной инфраструктуре с особым вниманием к АЭС страны[33]. Некоторые страны также проводят учения по реагированию на уже имевшие место кибер-кризисы. Так, Президент Южной Кореи, Пак Кын хе, отдала приказание о проведении учений и тренинга в условиях приближенных к возможной кибер-войне для всего персонала корейских гидроэлектростанций и АЭС после того, как в сетях этих предприятий было обнаружено вредоносное ПО[34].

Кроме прочего, международные учения помогают протестировать возможности реагирования в рамках симулирования международного сотрудничества в преодолении кризисов. Так, США раз в два года проводят учения «Кибер Шторм» (Cyber Storm), цель которых – повысить готовность к кризисным ситуациям государственного и частного секторов. Каждые учения Кибер Шторм основываются на ранее извлеченном опыте в рамках реальных инцидентов. Предполагается, что, разрешая имевшие место кризисные ситуации, участники будут готовы к действиям в еще более сложных случаях. В учениях «Кибер Шторм 2016» будут принимать участие представители шестнадцати штатов, одиннадцати государств, а также четырнадцати федеральных агентств[35]. Европейский Союз также раз в два года проводит учения «Кибер Европа» (Cyber Europe) по преодолению кризисов с участием стран-членов ЕС и представителей частного сектора[36]. Во время последних таких учений в 2014 году, продолжавшихся 24 часа, практически все страны ЕС имели возможность проверить свою готовность к почти двум тысячам кибер-атакам в режиме реального времени, включая такие как DDoS-атака, уничтожение или эксфильтрация данных, а также кибер-атаки против критических элементов инфраструктуры[37]. Кроме этого, Европейское оборонное агентство (EDA) и Североатлантический оборонный альянс (NATO) также проводят региональные комплексные учения по преодолению кибер-кризисов с целью повышения готовности стран-участниц к возникновению непредвиденных и сложных ситуаций, а также отработки трансграничного взаимодействия[38]. США и Великобритания заявили о том, что они проведут проверку того, как финансовые центры по обе стороны Атлантики будут

реагировать в случае совершения массированных кибер-атак. Учения прошли в ноябре 2015 года, и в их ходе была проведена проверка готовности стран и трансатлантической координации действий и коммуникаций[39].

Национальные КРКБ могут также использоваться в качестве механизма упрочения доверия между странами и развития межнационального сотрудничества. Так, Китай, Япония и Корея – страны, исторически испытывающие различные политические трения – создали и проводят раз в год трехсторонние встречи представителей национальных КРКБ для обсуждения и планирования механизмов кризисного реагирования. Такие встречи помогли в упрочении взаимного доверия и создания «горячей линии» для оповещения партнеров о значительных кибер-инцидентах[40].

Возможности и потенциал реагирования, совместные встречи и учения являются всего лишь немногими из широкого набора механизмов, которые могут помочь странам эффективно готовиться к кибер-кризисам и максимально минимизировать их последствия. КРКБ помогают повысить скорость и эффективность реагирования стран в случае кризисов, снижая общий экономический и оперативный ущерб от атак, проводимых на национальном уровне. Одними из основных условий эффективного функционирования таких команд являются высокое качество обучения персонала и наличие высококачественных инструментов быстрого реагирования и развертывания. Все это облегчает работу команд и повышает их способности в деле сотрудничества и координации по предотвращению и быстрому реагированию на кризисы, а также способствует более активному и эффективному обмену информацией между заинтересованными сторонами, как в самой стране, так и в международном масштабе.

Среди основных элементов действующей системы готовности к кризисам должны присутствовать:

Заявление:

A. Публикация плана реагирования на кибер-кризисы и инциденты;

B. Определение и визуализация кросс-секторных взаимозависимостей, которые влияют на поддержание деятельности сервисов и эффективность механизмов реагирования;

C. Обеспечение должного функционирования плана (учения, тренировки) и его регулярного обновления;

D. Публикация и распространение оценки кибер-угроз коммуникационным сетям Правительства, критически важных элементов инфраструктуры, и необходимым службам;

Организационные вопросы:

A. Создание национального КРКБ для управления механизмами реагирования в случае кризисов и инцидентов, а также оказания услуг широкому спектру клиентов в национальном масштабе (помимо Правительства и критически важных инфраструктур);

B. Идентификация авторитетных «контактных точек» в государственных и регулирующих органах;

C. Идентификация авторитетных «контактных точек» в критически важных предприятиях, несущих ответственность за деятельность и/или восстановление деятельности в экс-

тремальных ситуациях критически важных сервисов и элементов инфраструктуры;

D. Разработка и запуск системы оповещения и предупреждения, которая может использоваться национальными центрами реагирования и предотвращения кризисов для эффективного и своевременного получения, распространения и передачи срочной информации;

Ресурсы:

A. Определение, запрос и выделение человеческих и финансовых ресурсов для эффективной реализации своих полномочий национальной КРКБ;

B. Определение возможностей дополнительного финансирования с целью запуска и регулярного тестирования системы раннего оповещения и предупреждения, а также для тестирования степени готовности страны к кибер-инцидентам и кризисам при помощи проведения учений по кибербезопасности;

Реализация:

A. Продемонстрированная способность локализации, управления, устойчивости и гибкого реагирования на кризисы, а также реализации процесса восстановления критически важных сервисов и элементов инфраструктуры;

B. Продемонстрированная национальными КРКБ способность своевременно информировать все заинтересованные стороны о кризисных ситуациях;

C. Наличие информации о постоянно ведущихся исследованиях в области анализа последних тенденций или типов информационных и кибер-инцидентов национального масштаба, с определением инициаторов, их тактик, применяемых техник и процедур для определения актуальных трендов; а также

D. Разработка и реализация систем (программ) регулярного тестирования и замеров степени готовности к кибер-инцидентам и кризисам посредством проведения национальных учений.

Результаты замеров и исследований в рамках этой категории основаны на данных национальных КРКБ, предоставленных подразделением КРКБ Университета Карнеги-Меллон[41], Европейского агентства безопасности сетей и информации (ENISA)[42], FIRST[43] и МСЭ. Дополнительно использовались первичные и вторичные информационные ресурсы, такие как сайты национальных КРКБ, новостные ресурсы, для определения наличия возможностей, финансирования и степени готовности стран. По мере того, как страны осознают необходимость и важность создания национальных КРКБ, дополнения в рамках этой категории будут отражать, отслеживать и оценивать данные развития.

3. КИБЕРПРЕСТУПНОСТЬ И ОХРАНА ПРАВОПОРЯДКА

Третья важная категория для оценки кибер-готовности страны – ее приверженность в деле защиты общества от киберпреступности. Киберпреступность не является вопросом только лишь национального масштаба. Она пересекает государственные границы и поэтому требует решений на международном уровне. Страны должны

продемонстрировать приверженность защиты своих обществ от киберпреступности на *международном* уровне. Чаще всего это проявляется в форме участия в международных форумах, посвященных борьбе с транснациональными киберпреступлениями, а также создании национальных законодательных и регулятивных механизмов для борьбы с киберпреступностью. Ответственные государственные и регулирующие органы, призванные осуществлять такую деятельность, должны четко определить, что является киберпреступлением и предоставить правоохранительным и другим государственным органам механизмы, экспертную помощь и необходимые ресурсы для обнаружения и законного преследования киберпреступников и киберпреступной деятельности.

Приверженность стран к двум международным конвенциям может продемонстрировать их серьезность в деле защиты обществ от киберпреступности: «Конвенция о киберпреступности» Совета Европы и «Соглашение о сотрудничестве в области обеспечения международной информационной безопасности» Шанхайской организации сотрудничества (ШОС). «Конвенция о киберпреступности» Совета Европы, известная также как Будапештская Конвенция, вступила в силу 1 июля 2004 года. Она предоставляет странам механизм гармонизации национальных законодательств в сфере противодействия киберпреступности и расширения сотрудничества правоохранительной деятельности в этой области[44]. Тем не менее, действенность Будапештской конвенции в некотором роде ограничена, т.к. она позволяет присоединившимся странам выполнять ее требования выборочно под предлогом того, что обязательное выполнение ее положений может явиться «нарушением суверенитета, основ безопасности, общественного порядка или других существенных интересов» страны[45]. С другой стороны, «Соглашение о сотрудничестве в области обеспечения международной информационной безопасности» ШОС, подписанное в 2009 году, и известное также как Екатеринбургское Соглашение, содержит принципы, соответствующие подходам в обеспечении правопорядка Будапештской Конвенции. Соглашение также имеет своей целью повышение качества законодательств и создание механизмов практического взаимодействия между сторонами с целью обеспечения международной информационной безопасности[46]. Подписывая эти международные документы, страны обязуются принять соответствующие национальные законодательные акты, развивать международное сотрудничество, а также бороться с преступлениями посредством облегчения их выявления, расследования их обстоятельств и преследования их как на территории своего государства, так и в международном масштабе. ИКГ 2.0 отдает должное странам, присоединившимся или ратифицировавшим к любому из этих договоров. Эти страны взяли на себя определенные обязательства и обязанности в рамках национального законодательства демонстрируя приверженность международной кооперации по данному вопросу.

Помимо международных механизмов, описанных выше, существуют и реализуются и другие международные, межнациональные и региональные подходы в области борьбы с киберпреступностью. Так, к примеру, Генеральная Ассамблея ООН (ГА ООН) приняла целый ряд резолюций по киберпреступности, как например, резолюции 2001 года «О борьбе с незаконным использованием информационных технологий» и 2003 года «О создании глобальной культуры кибербезопасности и защиты критически важных элементов инфраструктуры»[47].

Так, Группа правительственных экспертов ООН (ГПЭ), которая состоит из представителей двадцати стран, пришла к чрезвычайно важному решению, когда ее участники согласились сотрудничать и совместно преследовать террористов и тех, кто незаконно использует ИКТ. Их приверженность в этом вопросе задокументирована в июньском 2015 г. отчете ГПЭ «О разработках в области информации и телекоммуникаций в контексте международной безопасности»[48]. АТЭС также реализовала проект в рамках расширения возможностей по борьбе с киберпреступностью, предоставив странам-членам возможности создать адекватные структуры и расширить возможности в деле расследования киберпреступлений. В рамках проекта более развитие страны АТЭС оказывают поддержку менее развитым государствам посредством обучения чиновников и следователей, работающих в указанной области[49].

ИКГ 2.0 оценивает кибер-готовность стан с точки зрения положений этих международных, межнациональных и региональных подходов. Кроме того, в оценке готовности страны используются также данные АСЕАН, МСЭ и других источников.

Однако, то, что государство артикулирует стремление бороться с киберпреступностью и ратифицирует международные соглашения в этой области, не всегда может означать реальную готовность бороться с киберпреступностью. Государства должны проводить серьезную работу для того, чтобы совершенствовать и развивать возможности правоохранительных органов в этой сфере. Так, к примеру, Центр исследований, разработок и обучения в области кибер-законодательства и судебной практики при Национальной школе права Бангалорского университета в Индии ведет активную работу «переводя» юридические нормы на язык технических терминов и обратно, предоставляя обучение и тренинги работникам судов, прокурорам, служащим следственных органов, персоналу обеспечивающему кибербезопасность, техникам, инженерам и многим другим. Этот Центр, финансируемый Департаментом электроники и информационных технологий (DeitY) Министерства телекоммуникаций и информационных технологий Индии, создал уникальные тренинги в рамках судебной лаборатории, которые оказывают реальную помощь участникам в понимании самых сложных юридических и технических вопросов и их взаимосвязи[50].

Еще одним положительным примером является запуск Международной организацией уголовной полиции (ИНТЕРПОЛ) Глобального инновационного комплекса ИНТЕРПОЛ (ГИКИ) в Сингапуре. Эта организация дает возможность офицерам правоохранительных органов сотрудничать с представителями ИТ-сектора для разработки новых методологий и инструментов в борьбе с киберпреступностью[51]. Так, в частности, эксперты ИНТЕРПОЛ создали игру-симулятор, которая помогает офицерам правоохранительных органов понять опасности и существующие взаимосвязи между Даркнетом (DarkNet) и криптовалютами. Даркнет создал огромный черный (незаконный) рынок, на котором продаются персональные идентификационные данные (ПИД), информация военных разведок, инструкции по сбору оружия и взрывчатых веществ, модульное вредоносное ПО, вредоносные программы zero day, персональные крипто-ключи и цифровые удостоверения личности, пароли к различным сервисам и множество другой нелегально полученной информации. Первый тренинг в рамках этой программы-симулятора был проведен ИНТЕРПОЛ в июле 2015 года[52].

Сокращение количества зараженных устройств, имеющих доступ в сеть – важный вклад в борьбу с кибер-преступностью.

Помимо расширения потенциала борьбы с киберпреступностью и возможностей правоохранительных органов, страны также должны прилагать усилия для очистки своих собственных сетевых инфраструктур, эффективно избавляясь от того, что получило название ботнетов[53]. В соответствии с экспертными оценками в настоящее время от 5 до 12% компьютеров в мире скомпрометированы как входящие в сеть ботнетов. По оценкам ФБР каждую секунду бонтет-армии заражают около восемнадцати компьютерных систем, принося тем самым ежегодные убытки мировой экономике на сумму в 110 миллиардов долларов[54]. Некоторые страны уже предпринимали некоторые шаги для минимизации этой угрозы, иногда достигая некоторого успеха. Так, проект Правительства Канады по углубленной аналитике и анализу DarkSpace для определения предиктивных индикаторов кибер-активности, реализуемый силами Bell Canada с участием команды экспертов правительственных агентств, исследовательских центров, а также представителей бизнеса, завершился созданием бизнес-кейса «чистые сети» - решения, которое содержало набор необходимых сведений для купирования и устранения угроз Канаде, поступающих из всемирной сети. На основе материалов проекта была создана национальная стратегия «чистые сети» и результаты оказали влияние на подготовку «Стандарта по кибербезопасности для поставщиков интернет-услуг»[55]. Еще один пример: в Японии с 2006 по 2011 годы национальный КРКБ (JP-CERT) создал и поддерживал работу Центра кибер-чистоты[56]. Этот Центр стал результатом кросс-дисциплинарного сотрудничества между JP-CERT, различными поставщиками услуг в области безопасности, а также интернет провайдерами. В рамках работы Центра была создана «охранная сеть» для противодействия активности ботнетов и их распространения. В дополнение, Центр разрабатывал индивидуальные способы решения проблем для отдельных вредоносных ПО в различных сетях и компьютерах[57]. Деятельность Центра кибер-чистоты впоследствии была продолжена компанией Telecom-ISAC Japan[58]. Наконец, в качестве примера можно привести австралийскую iCode, государственно-частное партнерство в рамках Австралийской инициативы для безопасного интернета (AISI), чьей целью является популяризация культуры безопасности в интернете среди провайдеров посредством снижения количества скомпрометированных устройств доступа в стране. iCode призывает всех австралийских провайдеров присоединиться к AISI и обеспечивает тех, кто это сделал, ежедневными данными о последних примерах вредоносного ПО и выявленных уязвимостях в сетях, ПО и устройствах[59].

Киберпреступность и мошенничество – это «налог» на экономический рост.

Киберпреступность и мошенничество – это «налог» на экономический рост. Убытки от киберпреступности достигли суммы в 445 миллиардов долларов в глобальном масштабе, с размером потерь в национальных ВВП от 1% и более, что

приводит к потере примерно 200 тысяч не созданных или утраченных рабочих мест[60]. Инвестиции в борьбу с киберпреступностью и развитие потенциала правоохранительных органов являются также и инвестициями в будущее развитие экономики страны. Развивая потенциал правоохранителей в борьбе с киберпреступниками посредством ратификации международных договоров, расширения международного сотрудничества, развития материальной базы, запуска анти-ботнет программ, а также других инициатив, страны могут значительно снизить свои риски и ускорить свой будущий экономический рост.

Среди основных элементов действенной системы приверженности защиты общества от киберпреступности должны присутствовать:

Заявление:

A. Озвученное стремление государства защитить свое общество от киберпреступности на национальном и международном уровне, выраженное посредством ратификации международных соглашений о борьбе с киберпреступностью, либо других соглашений, эквивалентных им;

B. Ясно выраженное намерение создать национальные правовые и политические механизмы снижения объемов криминальной деятельности в стране, а также создавать и развивать механизмы противодействия киберпреступности на национальном и международном уровне;

Организационные вопросы:

A. Создание серьезного институционального потенциала в области борьбы с киберпреступностью, в т.ч. повышение квалификации судей, прокуроров, юристов, правоохранительных органов и других специалистов;

B. Создание координирующего органа, чьей основной задачей будет являться обеспечение соответствие всех национальных стандартов, политик и т.п. международным требованиям (включая практику международного сотрудничества);

Ресурсы:

A. Выделение финансовых и человеческих ресурсов, требуемых для успешной борьбы с киберпреступностью;

B. Создание механизма отчетности, позволяющего определить, какая доля ВВП страдает от деятельности киберпреступников (а также фактические потери в национальной или одной из резервных валют) для того, чтобы оценить возможные грядущие затраты/выгоды и соответствующим образом спланировать инвестиции и выделение средств;

Реализация:

A. Продемонстрировать готовность страны пересмотреть и усовершенствовать законодательство и регулятивные механизмы, определить наличие пробелов в законах и областей пересечения полномочий, а также определить области, в которых модернизация требуется в первую очередь (напр. устаревшие законы в области телекоммуникаций и т.п.);

B. Составление списка действий, которые в рамках национального законодательства будут считаться уголовно-наказуемыми

деяниями в отношении таких явлений, как кража конфиденциальной информации, «кража личности», нарушение целостности компьютерных систем, сетей, баз данных, а также нелегальное использование таких систем, сетей и данных, в том числе с нарушением авторского права; и

C. Продемонстрировать эффективность деятельности страны в области сокращения количества и активности киберпреступлений, совершаемых на территории страны, и происходящих из инфраструктуры и сетей, находящихся на ее территории (в т.ч. создание анти-ботнет сетей и организация инициатив по выявлению и нейтрализации вредоносного ПО).

Оценка успешности страны в этой категории будет основываться на том, ратифицировала ли страна Будапештскую Конвенцию или Екатеринбургское Соглашение ШОС, и является ли страна активным участником региональных или межнациональных инструментов или политик, имеющих целью противодействие киберпреступности. Кроме того, оценивается и уровень ботнет-деятельности (как наличие узлов ‹управления и контроля›, так и общее количество зараженных устройств) с территории стран с целью определения степени эффективности анти-ботнет инициатив правительств. В рамках написания ИКГ 2.0 использовались первичные и вторичные источники для выяснения того, какие правовые и регулятивные механизмы созданы в стране, какие другие виды деятельности по снижению рисков проводятся на ее территории, а также какие ресурсы выделяются на обеспечение безопасности. Существенные и значительные изменения по данной категории будут тщательно отслеживаться, оцениваться и включаться в отчет.

4. ОБМЕН ИНФОРМАЦИЕЙ

Четвертой категорией, определяющей кибер-готовность страны, является ее способность создать и поддерживать функционирование механизмов обмена информацией, которые позволят обеспечивать эффективное взаимодействие и обмен важными сведениями между Правительством и бизнесом. Ключевая деятельность, такая как выявление, оценка и реакция на целевые атаки, которые могут иметь серьезные последствия для глобальных телекоммуникаций, торговли и деловых операций, требует гораздо большего, чем обычный мониторинг и применение традиционных защитных механизмов. В глобальном масштабе, большинство Правительств, организаций и бизнесов создали и используют программы обмена информацией для лучшего понимания угроз исходящих от официальных и неофициальных игроков, а также управления своим потенциалом по устранению уязвимых мест и исправления последствий заражения вредоносным ПО и взломов.

Обмен информацией должен производиться на основе доверия и взаимных обязательств всех заинтересованных сторон.

Формальные механизмы обмена информацией, подобные тем, которые создаются национальными КРКБ и ККР, могут значительно повысить

степень координации действий в случае реагирования в кризисной ситуации, облегчить обмен информацией об угрозах и развединформацией в режиме реального времени, а также повысить понимание того, какие секторы экономики находятся под угрозой, какая информация была утеряна в ходе инцидента, и какие средства и методы могут использоваться для защиты информационных активов. Существуют как минимум четыре модели реагирования на кибер-угрозы и защиты всеми заинтересованными своих информационных активов: 1) инициированная Правительством; 2) инициированная секторными предприятиями; 3) инициированная НПО; и 4) гибридная модель, инициированная и созданная при сотрудничестве Правительства, предприятий, НПО и исследовательских центров. У каждой из этих моделей есть свои достоинства и недостатки, такие, например, как необходимость сбалансировать своевременный обмен актуальной информацией о ситуации в области кибербезопасности с необходимостью охранить конфиденциальность данных, защитить гражданские свободы, а также грамотно распорядиться часто соревнующимися людскими и финансовыми ресурсами или интересами сторон. Тем не менее, для успеха каждой из моделей важны два фактора: доверие и взаимные обязательства всех сторон, что должно обеспечиваться четко артикулированными целями и задачами, ролями, ответственностью сторон и ожидаемыми результатами. Если говорить проще, если одна из сторон участвует в сотрудничестве с неохотой или ‹из-под палки›, положительного результата не достичь[61].

Более того, все заинтересованные стороны должны иметь возможность обмениваться всей имеющей ценность информацией о серьезных инцидентах, что предполагает наличие четких определений того, какого рода информацией они могут и должны обмениваться, кто будет иметь доступ к такой информации, а также какие защитные меры будут применяться в отношении этой информации после ее предоставления владельцем остальным сотрудничающим сторонам. Сложность процесса обмена такой чувствительной информацией возрастает пропорционально с ростом группы заинтересованных и участвующих в обмене сторон и, пожалуй, экспоненциально в случаях, когда участниками такой группы являются суверенные государства со своими определенными национальными интересами.

Многие страны уже разработали и внедрили надежные национальные программы обмена информацией, которые могут использоваться как удачные примеры другими странами. Эти программы обычно сосредотачиваются на распределение всех похожих игроков по группам и затем сведение всех этих групп в единую программу сотрудничества. В Нидерландах, к примеру, создан Национальный центр кибербезопасности (НЦКБ) – инициатива Правительства, которая возникла на основе голландского правительственного центра GOVCERT и превратилась в успешное государственно-частное партнерство, которое несет ответственность за кибербезопасность и обмен информацией в стране[62]. Одна из задач центра – постоянный мониторинг всех (потенциальных) источников угрозы в интернете и своевременное оповещение властей и заинтересованных организаций в случае обнаружения реальности такой угрозы. НЦКБ также напрямую связан со всеми Центрами обмена и анализа информации (ЦОАИ) в стране. Обмен информацией производится с использованием Traffic Light Protocol (TLP), с классификацией информации по четырем уровням конфиденциальности: красный, желтый, зеленый и белый. Нидерландская программа

обмена информацией была создана по образу британского Национального центра координации безопасности систем инфраструктуры (NISCC), который консультировал национальный бизнес в Великобритании по вопросам информационной безопасности[63]. Похожая ситуация и в Японии, где Агентство развития информационных технологий (АРИТ) действует как орган власти, наделенный полномочиями регулировать обмен информацией между Правительством и предприятиями критически важных секторов экономики. Это агентство продемонстрировало отличные результаты работы и сумело наладить доверительные отношения со всеми крупными предприятиями страны, одновременно делясь с ними ценными и важными релевантными разведданными и результатами анализа. Кроме того, АРИТ тесно сотрудничает с Министерство экономики, торговли и промышленности, национальным центром информационной безопасности и Команде по консультациям и экстренной кибер-помощи (J-CRAT) в деле преодоления всех крупных инцидентов, могущих вызвать ущерб для важных элементов национальной инфраструктуры[64].

В США, напротив, Центр обмена и анализа информации о финансовых услугах (FS-ISAC) является бизнес-инициативой, разработанной финансовыми институтами для определения, предотвращения и реагирования на кибер-инциденты и мошенничество в сети. Этот центр наработал тесные связи с поставщиками финансовых услуг; коммерческими компаниями, предоставляющими услуги в области кибербезопасности; федеральными, национальными, местными властями и властями штатов; правоохранительными органами; а также с другими пользующимися доверием и авторитетом организациями. Центр предоставляет своевременные и надежные оповещения о потенциальных угрозах своим партнерам по всему миру. Помимо прочего, FS-ISAC использует особую версию TLP для того, чтобы определять какие игроки могут и должны получать соответствующую информацию[65]. FS-ISAC расширяет свою сеть партнерства по обмену информацией на международный уровень, включая в нее организации из Великобритании и Европы. Подобные центры обмена и анализа информации существуют и в других секторах, не только в финансовом, однако они менее эффективны.

Национальный альянс кибер-экспертизы и обучения (NCFTA) США является некоммерческой корпорацией, чьей целью является облегчение сотрудничества между частными компаниями, исследовательскими центрами и правоохранительными органами в области определения, минимизации и нейтрализации комплексных кибер-угроз. Помимо представителей государственных органов, правоохранительных ведомств и бизнеса, это некоммерческое партнерское предприятие также работает на международном уровне, работая с представителями Канады, Австралии, Великобритании, Индии, Германии, Нидерландов, Украины и Литвы. Для обеспечения снижения уровня рисков и противоправных действий, NCFTA обеспечивает прямой и своевременный обмен информацией и аналитикой о кибер-угрозах с корпорациями и другими партнерами, а также с экспертами в различных секторах: НПО, частный бизнес, правоохранительные органы, исследовательские организации. Кроме того, альянс помогает в сборе необходимой информации для преследования преступников по закону[66].

Наконец, норвежский Центр кибер-информации и безопасности (ЦКИБ) при Университете Йёвика является совместной инициативой (исследователи, Правительство и бизнес-круги) и пред-

Актуальная и практическая информация – ключевой фактор уменьшения кибер-угроз.

ставляет еще один подход к обмену информацией и сотрудничеству в области кибербезопасности. ЦКИБ поддерживает единый в рамках страны подход в области информационной и кибербезопасности, а также разработал и использует схему обмена информацией для обеспечения возможностей общества определить, подготовиться и справиться с серьезными кибер-кризисами и инцидентами. Кроме того, он оказывает поддержку исследованиям и разработкам в области кибербезопасности.

Помимо различных программ обмена информацией, которые разрабатывают разные страны, происходит также сбор информации, связанной с кибербезопасностью, различными разведывательными и военными ведомствами в этих странах. Многие из таких организаций уже начали снимать гриф секретности с собираемой ими информации этого рода и делится ею не только с органами власти, но и представителями бизнеса. Действительно, своевременное информирование всех заинтересованных зачастую – важнейший элемент предотвращения или снижения остроты кибер-угроз. Некоторые страны, такие как Бразилия, разработали механизмы де-классификации (снятия грифа секретности) с актуальной информации, имеющей важность для безопасности других организаций (государственных и негосударственных), такие как их слабые места, относящиеся к ним угрозы, а также возможные тактики и способы преодоления таких угроз[67]. Повышение кибер-обороноспособности страны является очень важной задачей и многие страны готовы к снижению уровня секретности информации для того, чтобы повысить уровень безопасности в обществе.

Способность страны наладить обмен своевременной, практической и аккуратной информацией между заинтересованными государственными и негосударственными организациями помогает устранить уязвимые точки и слабые места, что впоследствии приведет к снижению уровня рисков. С ростом частоты и качества обмена информацией все участвующие в этом процессе организации оказываются способны более быстро и эффективно справляться с угрозами их сетевым инфраструктурам. Создание и поддержание программ обмена актуальной информацией является фундаментальной инвестицией в будущий экономический рост.

Среди основных элементов действенной национальной системы обмена актуальной информацией должны присутствовать:

Заявление:

A. Формализация и распространение положений о политике обмена информацией между различными секторами общества и экономики, которая позволит наладить эффективный обмен информацией и аналитикой между правительствами и соответствующими секторами экономики;

Организационные вопросы:

A. Определение ответственной организации, которая будет заниматься передачей достоверной информации от правительственных источников правительственным агентствам

и критически важным предприятиям (уровень Правительство-Правительство);

B. Определение ответственной организации, которая обеспечит реализацию механизма (формат и схема отчетности, технологии и проч.) обмена информацией между различными секторами общества и экономики (во всех направлениях), как актуальной (в режиме реального времени), так и юридически-процессуальной (пост-фактум) (уровень Правительство – предприятия / предприятия-предприятия);

C. Создание исследовательского центра или некоммерческого механизма для обмена информации об уязвимостях, инцидентах или кризисных решениях (альтернативная модель, например, NCFTA или Национальная база данных инфраструктурных уязвимых мест)[68];

Ресурсы:

A. Определение и выделение необходимых человеческих и финансовых ресурсов, требуемых для реализации схемы обмена актуальной информацией инициируемой Правительством, либо для любой другой формы или структуры такого обмена;

Реализация:

A. Продемонстрировать, что кросс-секторный и межорганизационные механизмы координации направлены на исправление проблем в критических областях, где существует взаимозависимость между двумя и более заинтересованными сторонами, включая оповещение о критических ситуациях и механизмы управления кризисными ситуациями на кросс-секторном и межорганизационном уровнях; а также, что эти механизмы поддерживаются на должном уровне эффективности и постоянно тестируются;

B. Продемонстрировать, что Правительство приняло и готово использовать процесс своевременной де-классификации (рассекречивания) аналитической и разведывательной информации по кибербезопасности, имеющей отношение к третьим сторонам, и предоставлять ее другим государственным органам и негосударственным организациям[69].

Оценка успешности страны в этой категории будет основываться на том, созданы-ли и действуют-ли в стране механизмы обмена информацией и координации действий. На основе информации из первичных и вторичных источников авторы ИКГ 2.0 определяют факт наличия таких механизмов и достаточность их финансирования. Существенные и значительные изменения будут тщательно отслеживаться, оцениваться и включаться в отчет.

5.ИНВЕСТИЦИИ В ИССЛЕДОВАНИЯ И РАЗРАБОТКИ

Пятой категорией, определяющей степень кибер-готовности страны, является определение кибербезопасности и более широких ИКТ инициатив как национальные приоритеты развития и инвестирование в теоретические и прикладные исследования в этих областях. Развитие ИКТ технологий революционизировало практически все сферы экономики, преобразовав предприятия, правительства, сферу образова-

ния, а также стиль жизни, работы и развлечений всего общества. Эти инновации являются двигателями экономического роста и могут значительно повысить потенциал общества, одновременно укрепив его безопасность.

Правительства и деловые круги каждый по-своему несут ответственность за результаты и финансирование исследований и разработок. Они могут объединить свои усилия и бюджеты для создания следующего поколения ИКТ, интернет-технологий и решений. Бизнесы и Правительства все активнее используют мобильный интернет, облачные вычисления, «большие данные», квантовые счисления, а также оборудованные выходом в сеть бытовые приборы и оборудование, и поэтому сами заинтересованы в инвестициях в безопасность и гибкость этих

трех компонентов. Первый, концентрируется на фундаментальных и прикладных исследованиях и называется «Превосходная наука» (Excellent Science). Среди задач этого компонента – финансирование двадцати пяти тысяч докторских исследований в ИТ в следующие семь лет. Второй компонент концентрируется на «Лидерстве в промышленных технологиях и их применении», с особым упором на ИКТ, нанотехнологии, новые материалы и их обработку. Третий компонент ставит своей задачей финансирование решений для социально-экономических проблем, например, в здравоохранении, энергетике, транспорте и безопасности. Один из критериев оценки качества инвестиций – это транснациональное сотрудничество между различными компаниями и решения, которые удовлетворяют и решают транс-европейские проблемы и задачи[70].

Исследования и разработки в области кибербезопасности должны способствовать доверию, безопасности и будущему развитию наших взаимосвязанных обществ.

цифровых услуг и технологий. Инвестируя в цифровые исследования и разработки, а также в другие инновации, страны, университеты или компании могут сократить свое отставание в возможностях защиты от кибер-атакующих лиц и организаций. Так, в рамках программы EC Horizon 2020 выделяется примерно 80 миллиардов Евро на исследования и разработку кибер-инициатив. Основываясь на принципах открытого доступа, эта программа стремится развивать и поддерживать реализацию результатов исследований, ускорить процесс создания инноваций, повысить их эффективность и прозрачность. Программа Horizon 2020 состоит из

Подобным же образом США выделяет, направляет и координирует ежегодные инвестиции в размере 4 миллиардов долларов в межотраслевые исследования в рамках Национальной программы информационных технологий, исследований и разработок (NITRD). Среди приоритетов на 2016-2020 годы: «большие данные» (big data), кибер-физические системы, исследования и разработки в области кибербезопасности и приватности, высокоскоростные вычисления, а также новые технологии беспроводного обмена данными[71]. Программа NITRD является основным источником самых современных технологий в области вычислений, сетевых техно-

логий и ПО в федеральном масштабе. Цель программы – ускорить развитие применение самых последних информационных технологий для упрочения национальной безопасности, а также повышения экономических возможностей и роста США. Кроме того, финансирование в кибер-исследования и разработки ведется и в рамках Проектного агентства современных оборонных исследований (DARPA), Агентства проектов современных исследований в области разведки и аналитики (IARPA), а также Агентства проектов современных исследований в области внутренней безопасности (HSARPA). Тем не менее, даже если все бюджеты на исследования и разработки всех этих организаций сложить вместе, они составят менее 1% ВВП США. Учитывая невероятно высокий уровень текущих и будущих кибер-рисков для США, 1% ВВП является неадекватной суммой для решения проблем в киберпространстве.

Другие инициативы, поддерживаемые правительствами, оказывают содействие развитию кибер-исследований и разработок, предлагая налоговые льготы или кредиты. Так, например, Израиль недавно узаконил серьезные налоговые послабления для компаний, работающих в области кибербезопасности в национальном технопарке Бэер-Шева исходя из того, что расширение объемов корпоративных и внутриорганизационных инвестиций зачастую требует стимуляции со стороны государства[72]. Поддерживая и развивая уникальную экосистему, в которой со-существуют и сотрудничают промышленники, исследователи, военные и правоохранители, Израиль тем самым создает стратегический и экономический центр безопасности. Технопарк Бэер-Шева также своим существованием стимулирует государственно-частное партнерство в области ИКТ, является центром разработки и внедрения инноваций, а также обеспечивает наличие эффективных образовательных программ и тренингов.

Еще одним рыночным механизмом развития образования, знаний и опыта в области ИКТ являются гранты и стипендии. Так, программа Правительства Бразилии «Наука без границ» предлагает учебные и исследовательские стипендии во всех областях технических и прикладных знаний, в том числе таких, как компьютерные исследования и ИТ. Подобным же образом поступает и Национальный совет научного и технологического развития (CNPq), агентство в составе Министерства науки, технологии и инноваций, которое выделяет стипендии «Для развития научных исследований», стимулируя развитие ИКТ знаний и опыта среди студентов[73].

Центры кибер-инноваций помогают превратить идеи и технологии в реальные решения.

Центры кибер-инноваций, такие, например, как Security Delta в Гааге (HSD), содействуют развитию инновационных исследований и разработок в ИКТ, а также развивают сотрудничество между частными компаниями, правительствами и исследовательскими организациями. HSD, это фонд финансируемый муниципалитетом Гааги и голландским Министерством экономики, который является крупнейшим европейским центром знаний и наработок в области безопасности, имеющим контакты и обменивающимся информацией и знаниями с такими же центрами в США, Канаде, Сингапуре и ЮАР. Среди его программ в области кибербезопас-

ности есть такие, как Академия кибербезопасности и Лаборатория исследований кибер-инцидентов. Среди текущих проектов – создание самой современной платформы обнаружения вредоносного ПО и разработка решений для определения, выявления и управления уязвимостями в ПО и архитектуре при помощи сканеров качества[74].

Частные «центры кибербезопасности» появились в Кремниевой долине, Тель-Авиве, Бостоне, Нью-Йорке и Лондоне. Так, лондонский центр инноваций, получивший название Cyber London (CyLon), является также первым Европейским центром поддержки и развития стартапов в области кибербезопасности. CyLon развивает экосистему кибер-инноваций в Лондоне и помогает становлению и развитию продуктов, обеспечивающих информационную безопасность[75].

Все эти инициативы и центры в области исследований и разработок позволяют ускорить преобразование идей и технологий в реальные решения, помогающие далее развивать цифровой рынок, повышать уровень безопасности на нем, а также развивать устойчивость сетей и инфраструктур, тем самым одновременно повышая уровень жизни населения.

Среди основных элементов приверженности страны к развитию исследований, образования и расширения собственных возможностей в области кибербезопасности должны присутствовать:

Заявление:

A. Публично озвученное обязательство Правительства инвестировать на национальном уровне в фундаментальные и прикладные исследования в области кибербезопасности;

B. Широко опубликованные механизмы стимулирования (напр., налоговые послабления) инновационных разработок в области кибербезопасности и их распространение в виде новых технологий, техник, процессов и инструментов;

C. Действующие правительственные механизмы стимулирования (гранты, стипендии) для поддержки и развития образования, создания новых знаний и развития опыта в области кибербезопасности;

Организационные вопросы:

A. Наделение полномочиями хотя бы одного органа для надзора и координации инициатив в области исследований и разработок, а также для функционирования в качестве контактной точки и центра международного сотрудничества;

B. Создание официально поддерживаемых учебных программ со степенями в области кибер- или информационной безопасности, или в подобных областях с упором на безопасность и устойчивость цифрового пространства;

C. Создание организации, чьей целью будет являться отслеживание и отчет по количеству и объему успешно претворенных в жизнь программ, финансируемых или поддерживаемых Правительством или бизнес сектором (от исследования к продукту/услуге) с особым вниманием тем решениям, которые реально повышают уровень

безопасности и устойчивости цифрового пространства;

Ресурсы:

A. Выделение человеческих и финансовых ресурсов, необходимых для фундаментальных и прикладных исследований и инициатив в области кибербезопасности;

B. Определение и выделение человеческих и финансовых ресурсов, необходимых для государственной или коммерческой передачи и реализации современных технологий и инноваций;

Реализация:

A. Реализация программ в области разработки, внедрения и повсеместного использования безопасных и совместимых стандартов безопасности, принятых и подтвержденных международными органами стандартизации;

B. Наличие свидетельства усилий Правительства в области поддержки, развития и стимулирования разработок и исследований в области кибербезопасности, особенно в области фактической реализации таких разработок в виде конкретных решений (т.е. процент таких разработок, реализованный и используемый в аппарате Правительства), а также доля решений, принятых и используемых на коммерческом уровне; и

C. Наличие свидетельств существования бизнес-инициатив в области кибербезопасности (напр. Центров/хабов кибер-инновации), в рамках которых поддерживаются и развиваются исследования и разработки, особенно в области фактической реализации таких разработок в виде конкретных решений (т.е. процент таких разработок, реализованный и используемый бизнесом), а также доля решений, принятых и используемых на уровне Правительства.

Оценка успешности страны в этой категории будет основываться на том, инвестирует-ли страна в исследования и разработку, образование, создание знаний и развитие навыков – наряду с более широким финансированием и поддержкой других инициатив в области кибербезопасности. На основе информации из первичных и вторичных источников авторы ИКГ 2.0 определяют факт наличия таких механизмов и достаточность выделенных ресурсов. Существенные и значительные изменения будут тщательно отслеживаться, оцениваться и включаться в отчет.

6. ДИПЛОМАТИЯ И ТОРГОВЛЯ

Шестой важной категорией определения степени кибер-готовности страны является степень ее вовлеченности в решения вопросов кибербезопасности как части ее внешней политики. На фундаментальном уровне кибер-дипломатия стремится найти приемлемые для всех решения общих проблем и вызовов. Вопросы, связанные с кибербезопасностью, возникают в большом количестве областей международных отношений, таких как права человека, экономическое развитие, торговые соглашения, контроль над распространением вооружений и технологий двойного назначения, безопасность, стабильность и мирное разрешение конфликтов. Несмотря на то, что вопросы безопасности так или иначе затрагиваются в ходе любых переговоров, а также то, что все их участники – экс-

перты в соответствующих областях по тематике переговоров (напр. торговля или контроль за нераспространением оружия), эти эксперты зачастую незнакомы с теми возможностями или рисками, которые привносит кибер-контекст в обычную тематику переговоров. Поэтому, создание отдельного отдела или наём специального персонала, в чьи дипломатические компетенции будут входить вопросы кибербезопасности, должно стать неотъемлемой частью внешней политики любой страны.

На фундаментальном уровне кибер-дипломатия стремится найти приемлемые для всех решения общих проблем и вызовов.

С учетом очень неспешного экономического роста или восстановления экономик, многие страны начинают реализовать новый вид международной политики, основанный на заключении торговых соглашений в качестве основного средства, стимулирующего рост. Одновременно, во время этих переговоров по вопросам экономического развития обсуждаются, порой неявно, и вопросы национальной безопасности. Так, 5 октября 2015 года было подписано соглашение о Транстихоокеанском партнерстве (ТТП). Цель этого соглашения – увеличить объемы торговли и инвестиций между странами-членами инициативы, развивать инновации, способствовать экономическому росту и развитию, а также способствовать созданию новых и сохранению старых рабочих мест. Для того, чтобы достичь согласия по этому документу, понадобилось пять лет, и частично – из-за вопросов кибербезопасности. Договаривающиеся стороны не могли договориться по ключевым вопросам, в т.ч. и по вопросам защиты данных и приватности (напр., защиты интеллектуальной собственности), подходов к локализации данных и ограничений по контенту.

США и ЕС в настоящее время ведут переговоры о Трансатлантическом торговом и инвестиционном партнерстве (ТТИП), которое во многом похоже на ТТП. Цели этого соглашения – увеличить доступ к рынкам стран, снять ненужные регулятивные препятствия на пути товаров, услуг и капиталов, установить четкие правила в области коммерческих взаимоотношений между организациями двух регионов, создать новые рабочие места и способствовать росту ВВП[76]. Два основных вопроса, из-за которых откладывается подписание документа – защита данных и приватность. В течение последнего десятилетия ЕС и США выработали общий подход в области единых стандартов защиты и передачи всех персональных данных, которые хранятся или передаются в/между США и ЕС[77]. Однако утечка документов Эдвардом Сноуденом раскрыла факт, что разведслужбы США собирали сведения о зарубежных правительствах и лицах, что привело к потере доверия между сторонами. В результате этого, многие государства ЕС требуют создания стандартов защиты данных, правил шифрования и законодательных норм на национальном уровне для того, чтобы самим идти в ногу с последними технологиями и иметь возможность возложить ответственность за адекватную защиту данных на правительства. Кроме того, Суд ЕС отменил действие соглашения ("Safe Harbor" agreement) о совместной защите

данных и стандартах между ЕС и США. Это соглашение позволяло американским компаниям автоматически получать сертификат для работы с данными пользователей из стран ЕС и «адекватно защищать» эти данные в соответствии с Директивой Еврокомиссии о защите данных и фундаментальными правами человека в Европе, в частности – в соответствии с правом на частную жизнь. Пока переговаривающиеся стороны занимаются уточнениями положений этого договора, переговоры по ТТИП не сдвинулись с места[78]. В настоящее время Торговая палата США в ЕС выступила с оценкой, что полная отмена соглашения о совместной защите данных будет стоить Евросоюзу до 1,3% ВВП[79].

Еще одно региональное соглашение о свободной торговле, Региональное всестороннее экономическое партнерство (РВЭП) в настоящее время находится в стадии переговоров среди стран-членов АСЕАН и представителей Китая, Индии, Японии, Республики Корея, Австралии и Новой Зеландии. Шестнадцать стран-участниц переговоров являются домом практически для половины населения планеты, производят почти 30% мирового ВВП и почти четверть глобального объема экспорта. Цель РВЭП – снизить или снять торговые барьеры, содействовать экономическому и техническому сотрудничеству, защитить интеллектуальную собственность, упростить урегулирование спорных вопросов, а также упростить доступ к рынкам для экспортеров товаров и услуг. В рамках этих переговоров некоторые страны стремятся включить в них вопросы защиты данных, заявляя, что суверенитет в области данных является вопросом национальной безопасности[80].

Кроме того, в настоящее время идет целая серия переговоров по вопросам безопасности, с особым упором на проблематику современных технологий. К примеру, Вассенарские соглашения о контроле экспорта обычных вооружений и товаров двойного назначения, которые подписаны 41 страной, в т.ч. США, Великобританией, Россией и большинством стран ЕС, недавно решили ограничить продажу «коммуникационных систем интернет-слежки» и «ПО вторжения», которые специально созданы или переработаны с тем, чтобы остаться незамеченными программами и инструментами мониторинга или уничтожить системы противодействия и защиты[81]. У государств-участников Соглашения присутствует серьезная озабоченность относительно возможного двойственного применения таких технологий. Так, инструмент оценки и определения уязвимостей зачастую использует «дыры» в ПО для обнаружения сетевых уязвимостей и слабых мест. Те же техники и методы могут использоваться и в качестве оружия. Поэтому установление экспортного контроля за такими технологиями отражает мнение, что современные технологии потенциально могут угрожать системам национальной обороны или представлять риск для национальной безопасности.

В рамках других идущих в настоящее время переговоров и дискуссий стороны пытаются прийти к общему пониманию или установить общие правила для повышения стабильности в глобальном ИКТ-пространстве. Это включает развитие механизмов сотрудничества в случаях кибер-инцидентов и получения ответов на запросы об ИКТ-инфраструктуре (к примеру, когда противоправная деятельность осуществляется с территории страны, где компьютеры заражены бот-вирусами). Дипломатия также используется для того, чтобы определить какие виды кибер-деятельности должны считаться законными, а какие – нет (напр., установление

стандартов ответственного поведения государств), что также известно, как *общепринятые нормы кибер-поведения*. Так, к примеру, недавно Группа Правительственных Экспертов ООН отметила, что ИКТ пространство носит глобальный характер, равно как и существующие в нем потенциальные угрозы, и призвала к сотрудничеству и совместным мерам в области преодоления таких угроз. Группа также отметила, что соблюдение международного законодательства, в частности – обязательств в рамках Устава ООН, дает достаточную основу для использования странами ИКТ. Эксперты согласились, что они приступят к созданию рамочных общих норм, правил или принципов ответственного поведения, а также мер по повышению взаимного доверия (МПВД)[82]. В рамках МПВД Группа согласилась обратить особое внимание на упрочение механизмов сотрудничества между ответственными государственными органами для того, чтобы успешнее решать проблемы с ИКТ-инцидентами, а также разработать дополнительные технические, законные и дипломатические механизмы для реагирования на запросы об ИКТ-сетях и инфраструктуре (напр. создать КРКБ или другую официальную организацию, которая бы взяла на себя эти обязанности). Совсем недавно Президент США Барак Обама и Председатель КНР Си Цзиньпин согласились (в принципе) следовать рекомендациям Группы Экспертов и придерживаться установленных ООН норм кибер-поведения, и в особенности – тех, которые касаются кибер-атак, стремящиеся нанести вред важнейшим элементам инфраструктуры оппонента в мирное время[83].

Кибер-безопасность – неотъемлемая часть всех компонентов внешней политики и торговли.

Учитывая некоторые рекомендации Группы, лидеры Бразилии, России, Индии, Китая и ЮАР (БРИКС) пришли к согласию сотрудничать друг с другом в преодолении общих ИКТ проблем. Они согласились обмениваться информацией и опытом в области безопасного использования ИКТ, координировать свою борьбу с киберпреступностью, создать контактную сеть между странами-членами организации, а также установить сотрудничество в рамках БРИКС на уровне КРКБ. Страны БРИКС также призвали международное сообщество сосредоточиться на создании и развитии МПВД, развитии технического потенциала, неиспользовании силы в конфликтах, а также на предотвращении ИКТ-конфликтов[84]. Более того, в январе 2015 года Шанхайская организация сотрудничества (ШОС) представила в Генассамблее проект пересмотренных правил кибер-поведения и ИКТ-безопасности, которые определяют права и обязанности стран в информационном пространстве, продвигают конструктивные и ответственные действия и подходы, а также упрочивают сотрудничество в области преодоления актуальных для всех ИКТ-рисков[85]. ШОС пересмотрела Правила поведения 2011 года и привела их в соответствие с отчетами Группы Экспертов от 2012 и 2013 годов для того, чтобы призвать как можно большее количество стран-членов Группы 77 присоединиться к кодексу ответственного поведения.

Другие международные альянсы и саммиты также соединяют темы экономики, развития и безопасности. К примеру, МСЭ проводит регулярные дискуссии по вопросам политики, технологии и регулирования ИКТ и интернета во

время четырех глобальных встреч: Всемирного саммита по информационному обществу (ВСИО), Всемирной конференции по развитию телекоммуникаций (ВКРТ), Всемирной конференции по международным телекоммуникациям (ВКМТ) и Всемирной ассамблеи по телекоммуникационной стандартизации (ВАТС)[86]. Кроме прочего, Организация американских государств (ОАГ) и Межамериканский банк развития (МАБР) объединили свои усилия с тем, чтобы вести систематическую работу со странами-членами по вопросам кибербезопасности в трех областях взаимодействия: (1) развитие с учетом социальной инклюзивности, а также устойчивости и охраны окружающей среды; (2) ИКТ как средство генерирования дохода и создания новых рабочих мест, получения доступа к информации и бизнес-возможностям, развития онлайн-обучения и развития госуслуг; а также (3) безопасность, основных инфраструктур и услуг для граждан[87].

Очевидно, что проблемы кибербезопасности все активнее появляются во все большем количестве дипломатических кругов и дискуссий. Кибербезопасность, это не только проблема безопасности; это – фундаментальный элемент торговли, международной и экономической политики, а также потенциала будущего экономического роста страны. Основными условиями для способности страны эффективно принимать участие в обсуждении вопросов ИКТ является воспитание и обучение мотивированного и знающего персонала, создание специализированных структур, а также выделение средств на проведение дискуссий и переговоров, посвященных кибербезопасности. Так, Израиль и Чехия разместили своих «кибер-атташе» в своих посольствах в ключевых столицах мира, включая Вашингтон и Брюссель[88].

Кроме того, надо упомянуть, что США провели недельный тренинг по кибер-вопросам для дипломатического персонала, командированного в страны Азии[89]. Создание, воспитание и обучение подобного персонала является все более важным фактором для страны в деле определения ее будущей внешней, экономической, торговой политики и целей экономического развития.

Основные элементы определения возможностей в области вовлеченности в кибер-тематику в дипломатии, включают:

Заявление:

A. Официальная констатация того, что кибербезопасность является важным элементом внешней политики и национальной безопасности страны (напр. эти вопросы обсуждаются на встречах высокопоставленных политиков и военных в двухсторонних и многосторонних форматах);

B. ИКТ и кибербезопасность объявлены важными элементами международной экономической политики, переговоров, а также торговли и коммерции;

Организационные вопросы:

A. Обучение специализирующегося на ИКТ тематике персонала во внешнеполитическом ведомстве страны или подобной организации, чьей основной задачей является активное участие в международной дипломатии по кибер-вопросам;

B. Заметное соответствие между числом и рангом дипломатического персонала разбирающихся в кибер-вопросах и заявлен-

ной приверженностью страны заниматься «кибер-дипломатией» как одной из главных тем национальной важности;

Ресурсы:

A. Определение потребности и выделение необходимых человеческих и финансовых ресурсов для полноценного участия страны в дипломатической деятельности по ИКТ-вопросам;

Реализация:

A. Явное участие в переговорах, подписании и ратификации международных, межнациональных, региональных и/или двусторонних соглашениях, предусматривающих приемлемые для всех сторон решения общих проблем; а также

B. Заметные усилия направленные на оказание влияния на международные торговые и коммерческие соглашения, связанные с использованием ИКТ или совместным использованием кибер-инфраструктуры, критических услуг и технологий в международном, региональном и/или национальном масштабе.

Оценка успешности страны в этой категории будет основываться на том, создало-ли или выделило-ли Правительство специальный отдел (орган), либо наделило особыми дипломатическими полномочиями своих представителей с учетом кибер-особенностей экономики и безопасности. На основе информации из первичных и вторичных источников авторы ИКГ 2.0 определяют, если и в какой степени такие органы или представители участвуют в, и оказывают влияния на, международных переговорах по вопросам кибербезопасности. Существенные и значительные изменения будут тщательно отслеживаться, оцениваться и включаться в отчет.

7. ОБОРОНА И КРИЗИСНОЕ РЕАГИРОВАНИЕ

Седьмая и последняя категория определения кибер-готовности страны – степень способности вооруженных сил государства, и/или подобного оборонного агентства или ведомства, защитить страну от угроз, исходящих из кибер-пространства. Страны, заинтересованные в такого рода возможностях, стимулируют создание в рамках своих вооруженных сил специальных подразделений или проводят учения для реагирования на угрозы, которые могут возникнуть и подняться до уровня национальных в случае «кибер-конфликта»[90].

Страны становятся все более взаимосвязанными и зависимыми от интернета, что, в свою очередь, делает их более уязвимыми от разрушительных и деструктивных кибер-атак. Оборонные инструменты и системы многих стран чрезвычайно слабы перед лицом сложных и продуманных кибер-атак. Взаимосвязанная природа глобальной конкуренции и конфликтов провоцируют противников, имеющих потенциал в кибер-сфере, фактически перейти национальные границы и системы и нанести удар по коммерческим и негосударственным организациям страны-противника. Так, в августе 2012 года компания Saudi Aramco подверглась нацеленной атаке с использованием вредоносного ПО, в ходе которой были разрушены базы данных и было уничтожено почти 75% ИТ-инфраструктуры компании[91]. Служащие компании заявили, что основной целью нападения было нарушение производства нефти. Несколько месяцев спустя, в марте 2013 года, многие финансовые

организации Южной Кореи, включая четвертый по величине банк в стране, Shinhan Bank, пострадали от вредоносного ПО, подобного тому, что использовалось против Saudi Aramco. Банковские интернет-услуги были прерваны, а базы данных оказались стерты. Экономический ущерб от этого инцидента оценивается в 800 млрд. долларов США[92]. В декабре 2014 года хакеры успешно проникли и взяли под контроль системы управления компании German Steel Mill, что привело к непредвиденной и некорректной остановке доменной печи компании, что, в свою очередь, привело к значительному ущербу[93]. В том же году компания Sony Pictures стала жертвой кибер-атаки, в результате которой были похищены копии еще не выпущенных на рынок фильмов, электронная почта украдена, а потом и ‹слита›, а финансовые документы были раскрыты. Были скопированы данные десятков тысяч служащих компании, и примерно 80% ИТ-активов компании (как ПО так и оборудования) – разрушены вредоносным ПО[94].

Подрывающие и разрушительные кибер-атаки требуют наличия надежной кибер-защиты.

Страны должны быть готовы защищать свои интернет-интересы в настоящих и будущих конфликтах. Скорость проникновения интернета во все аспекты жизни общества дает доступ к этим аспектам новейшему кибер-оружию, что приводит к ассиметричным выгодам для слишком многих сторон. Действительно, разнообразие тех, кто готов на разрушительные действия, поражает: политические активисты, преступники, террористы, государственные и негосударственные организации. У всех у них различные мотивы, и это заставляет готовиться к различным худшим сценариям. В настоящее время уже более шестидесяти стран разработали возможности и инструменты для кибер-шпионажа и нападения, одновременно демонстрируя интерес к приобретению или разработке оборонных и упреждающих/нападающих средств и инструментов[95]. Более того, страны приступили к разработке различных стратегий и инструментов для повышения своих национальных уровней кибер-обороноспособности. Большинство правительств инстинктивно стремятся расширить существующие оборонные возможности своих органов безопасности, которые уже в состоянии действовать, насколько позволяет интернет, вне границ своего государства (напр. агентство обороны или разведки). Другие государства стремились предоставить такие возможности организациям, не относящимся напрямую к их системе обороны[96].

Так, в 2010 году США создали специализированное подразделение – Кибер-командование США (United States Cyber Command) – для защиты от кибер-угроз военной инфраструктуре. Полномочия Командования были расширены в 2015 году, когда Департамент обороны (ДО) опубликовал вторую редакцию Кибер Стратегии, которая предусматривала создание кибер-сил ДО США (под руководством Кибер-командования) для упрочения кибер-обороны и кибер-защиты государства. Эта новая стратегия констатирует необходимость быть готовыми «защищать территорию США и их жизненные интересы от разрушительных или деструктивных кибер-атак, могущих иметь серьезные последствия», а также создание, реализация и запуск средств, могущих контролировать эскалацию конфликтов и влиять на развитие событий на всех этапах конфликтов[97].

Подобным же образом в декабре 2014 года Россия опубликовала новую Военную доктрину, в которой констатируется намерение развивать кибер-возможности как для оборонных целей, так и для целей нападения, а также создания системы «не-ядерного сдерживания»[98]. Белая книга Минобороны России от 2011 года, озаглавленная «Концептуальные вопросы деятельности Вооруженных сил Российской Федерации в информационном пространстве», созвучна аспектам Российской оборонной доктрины, однако также содержит положения об учете общественного мнения и необходимости держать СМИ в курсе происходящего с целью сохранения возможности де-эскалации конфликта[99]. По сообщениям российских СМИ, российское руководство планирует опубликовать новую Доктрину информационной безопасности в 2016 году, которая предложит разработку сил для информационной войны и информационных систем стратегического сдерживания и предотвращения конфликтов[100].

Южная Корея и Бразилия также создали подобные военизированные соединения, целью которых является создание возможностей для предотвращения, отражения и ответа на кибер-атаки, а также обеспечение полной и безоговорочной победы в случае кибер-войны[101]. Южная Корея постоянно расширяет свои кибер-ресурсы и возможности и, по последним сообщениям, обучает около 400 военных для кибер-командования сил обороны, чтобы довести их число до тысячи[102].

Хотя Китайская Народная Республика (КНР) и не публиковала официально какую-либо стратегию или доктрину в области кибер-конфликтов или информационно-военных вопросах, опубликованные Основные направления военной стратегии содержат рекомендации по оборонной политике[103]. Белая книга КНР от 2013 года «О различных функциях Вооруженных сил Китая» и «Мнение об усилении работы в области информационной безопасности» от 2014 года, подчеркивают развитие возможностей страны в области кибер-обороны. Документы подчеркивают, что Народно-освободительная армия (НОА) не будет нападать первой, но в случае нападения на нее, нанесет ответный удар и в киберпространстве[104].

Орган или агентство кибер-обороны не обязательно должны входить в состав вооруженных сил страны. Национальная полиция и органы безопасности (разведки) могут стать центральными компетентными органами Правительства в деле обороны в киберпространстве, хотя, конечно, Вооруженные силы также должны быть модернизированы и подготовлены к действиям в киберпространстве в случае вооруженного конфликта. Например, Исландия решила сконцентрировать свои силы кибер-реагирования вне своих Вооруженных сил. В прошлом, обязанности в области кибер-безопасности были там распределены между Министерством внутренних дел, Администрацией почты и телекоммуникаций, Агентством защиты данных и Полицией Исландии. Однако, в 2015 году Исландия централизовала свои мощности в области кибер-обороны под руководством Национального комиссара Полиции Исландии[105]. Национальная кибер-стратегия Исландии от 2015 года также отмечает важную интегральную роль НАТО в структуре национальной кибер-защиты страны[106].

Наконец, несмотря на то, что формально у Израиля сегодня нет «кибер-командования», у него все же есть возможности в области кибер-обороны, которые распределены между Силами обороны Израиля (СОИ) и Директоратом военной разведки. Директорат занимается наступа-

тельными кибер-операциями, в то время как службы безопасности ответственны за оборону. Шин-бет (или Шабак), служба государственной безопасности Израиля, несет ответственность за защиту государственных систем и критически важных элементов национальной инфраструктуры, а Национальные кибернетические силы защищают критически важные сети и частные предприятия от хакеров и шпионажа[107]. Однако эта ситуация может поменяться, потому что в июне 2015 года генерал-лейтенант Гади Айзенкот, Главнокомандующий Армии Израиля, заявил о своем намерении создать новый Корпус обороны Израиля, ответственный за кибер-оборону, наряду с Военно-морским и Военно-воздушным корпусами. Если Министр обороны одобрит идею нового корпуса, кибер-корпус обороны Израиля приступит к службе через два года после такого одобрения. После начала своей работы, новое кибер-командование интегрирует оборонные задачи и возьмет на себя обязанности по электронной разведке и обороне, в настоящее время выполняемые Командой 8200 и другими органами армейской разведки[108]. Это соответствует новому пятилетнему плану развития Сил обороны Израиля, «Гидеон», опубликованному в августе 2015 года. «Гидеон» содержит планы по активизации деятельности в области отражения кибер-атак и других ассиметричных угроз, которые могут исходить от негосударственных и террористических групп в регионе[109].

Кибер-оборона является необходимым фактором для обеспечения национальной и экономической безопасности. С ростом зависимости стран от интернета и ИКТ-систем, тем более уязвимыми они становятся в отношении «низовых» угроз и ассиметричных атак. То есть, страны, фактически, сталкиваются с Уловкой-22, когда все большее количество ИКТ-возможностей необходимы для дальнейшего роста, однако с ростом зависимости от интернета и технологий растет и масштаб рисков. Отказ от интернет-экономики в наше время уже не является серьезным вариантом. Страны должны быть готовы защищать себя в киберпространстве. Если страна неспособна себя защитить, нельзя говорить о ее кибер-готовности.

Элементами определения приверженности страны к развитию и разворачиванию национальных систем и органов кибер-защиты, являются:

Заявление:

A. Публикация национальных заявлений, в которых какому-то органу дается миссия по обеспечению кибер-защиты как приоритет его деятельности;

B. Формулирование политических полномочий и стратегий для данного органа кибер-защиты, которые позволяют реагировать на кибер-угрозы;

C. Заявления на национальном уровне, которые позволяют органу кибер-защиты развивать свои возможности реагировать на угрозы, как на суверенной территории страны, так и за ее пределами;

Организационные вопросы:

A. Создание национального органа, в рамках Вооруженных сил, чьей основной целью является кибер-оборона страны;

B. Создание национального органа, вне Вооруженных сил, чьей основной целью является кибер-оборона страны;

Ресурсы:

A. Определение потребности и выделение необходимых человеческих и финансовых ресурсов для органа в рамках Вооруженных сил, чья миссия ясно включает кибер-оборону страны;

B. Определение потребности и выделение необходимых человеческих и финансовых ресурсов для органа вне Вооруженных сил чья миссия ясно включает кибер-оборону страны;

Реализация:

A. Свидетельства того, что на уровне Правительства проводятся учения, обеспечивающие национальную кибер-готовность;

B. Свидетельства того, что на национальном уровне проводятся учения с участием частных предприятий, могущих находиться под угрозой, что обеспечивает национальную кибер-готовность;

C. Свидетельства того, что проводятся учения с участием международных партнеров (напр. сил совместной обороны НАТО или Азиатско-Тихоокеанской команды быстрого компьютерного реагирования (APCERT)), которые демонстрируют готовность страны к сотрудничеству посредством обмена информацией и помощью;

D. Создание стандартов ответственного поведения страны в киберпространстве и определение порогов, которые сделают применение сил кибер-защиты возможными для страны; а также

E. Создание механизмов быстрого реагирования (отдельно от КРКБ или их аналогов) для Правительства или отдельных секторов экономики в случае серьезных кибер-инцидентов.

Оценка успешности страны в этой категории будет основываться на том, объявила ли страна официально о создании сил обороны с основной задачей кибер-обороны государства. На основе информации из первичных и вторичных источников авторы ИКГ 2.0 определяют состояние дел в этой сфере. Существенные и значительные изменения будут тщательно отслеживаться, оцениваться и включаться в отчет.

ЗАКЛЮЧЕНИЕ

На сегодняшний день ни одна из стран не находится в состоянии кибер-готовности.

Угрозы нашим сетевым системам и инфраструктуре реальны и становятся все более серьезными. Они вызывают серьезные расходы и возможные убытки для стран и обществ. Экономические и национальные повестки дня должны соединиться с тем, чтобы привнести большую прозрачность в вопросах *кибер-небезопасности*. Понима-

ние этой важной взаимосвязи может подстегнуть интерес на национальном и глобальном уровнях к потенциальным экономическим потерям. Сравнительная, всеобъемлющая и основанная на широком опыте методология ИКГ 2.0 предоставляет набор параметров для определения зрелости и приверженности страны в области сохранения и обороны своих национальных инфраструктур и критически важных услуг, от которых зависит их будущее развитие.

Набор параметров ИКГ 2.0 включает в себя более 70 уникальных индикаторов в рамках семи категорий: национальная стратегия, системы реагирования, киберпреступность и охрана правопорядка, обмен информацией, инвестиции в исследования и разработку, дипломатия и торговля, а также оборона и кризисное реагирование. Эти индикаторы и категории предоставляют странам рамочный подход для развития более мощной системы обеспечения безопасности, которая сможет защитить страну от эрозии ВВП. Фактически, ИКГ 2.0 бросает вызов традиционному мнению, что кибербезопасность в основном является частью вопроса национальной безопасности. ИКГ 2.0 показывает, насколько сильно национальная безопасность связана с развитием интернета и ИКТ, которые, при условии обеспечения безопасности, ведут к экономическому росту и процветанию.

Вместо стандартного изучения проблемы, авторы ИКГ 2.0 предлагают странам рамочные подходы оценки их способностей предотвратить экономические потери в связи с кибер-угрозами. ИКГ 2.0 будет периодически обновляться и дополняться посредством добавления критериев оценки без потери сравнительной ценности по сравнению с предыдущими версиями. Таким образом, ИКГ 2.0 отразит прогресс стран и их развитие по пути к обеспечению безопасности их инфраструктур и услуг, от которых зависит их цифровое и экономическое будущее.

Ни одна страна не может себе позволить пренебрежение кибер-безопасностью и те потери, которые она вызывает. Данные, содержащиеся в ИКГ 2.0 и методология отчета могут оказать содействие лидерам стран проложить путь к более безопасной и устойчивой экономике во все более кибернетизированном, конкурентном и подверженном конфликтам мире.

Чтобы узнать больше или предоставить данные для ИКГ 2.0, обращайтесь по адресу: CyberReadinessIndex2.0@potomacinstitute.org

ОБ АВТОРАХ

Мелисса Хатауэй (Melissa Hathaway) – ведущий эксперт в вопросах кибербезопасности и политики киберпространства. Работает старшим научным сотрудником и является членом совета директоров Потомакского института политических исследований, а также Старшим советником Центра наук и международных отношений Бэлфер колледжа Кеннеди в Гарвардском университете. Кроме того, она является Почетным научным сотрудником канадского Центра инноваций международного управления и получила назначение в состав Глобальной комиссии по управлению интернетом (комиссия Бильдта). Работала с двумя президентскими администрациями США, в т.ч. была основным автором Обзора политики в области киберпространства для Президента Барака Обамы и руководила Общей национальной инициативой по кибербезопасности при Президенте Дж. Буше-мл. Является разработчиком уникальной методологии оценки и замеров уровня готовности к определенным кибер-рискам, известной как Индекс кибер-готовности. Регулярно публикует исследовательские статьи по вопросам кибербезопасности в отношении стран и компаний. Статьи можно прочитать по адресу: http://belfercenter.ksg.harvard.edu/ experts/2132/melissa_hathaway.html.

Крис Демчак (Chris Demchak) - эксперт проекта Индекс кибер-готовности Потомакского института политических исследований. Сферы научного интереса: кибер-устойчивость, кибер-конфликты, а также структуры и риски в киберпространстве. Является создателем и автором компьютеризированной организационной модели «Атриум», которая помогает крупным предприятиям выявлять и нивелировать непредвиденные проблемы в их цифровых системах. Также является автором книги «Войны на устойчивость и разрушение: кибер-конфликты, власть и национальная безопасность»

Джейсон Кербен (Jason Kerben) - эксперт проекта Индекс кибер-готовности Потомакского института политических исследований. Также работает в качестве старшего советника во множестве агентств и департаментов по вопросам, связанным с информационной и кибер-безопасностью. В частности, в сфере его научных интересов – законы и регулятивные подходы, которые оказывают влияние на миссию предприятия или организации. Разрабатывает методологии и подходы в оценке и управлении кибер-рисками и консультирует по множеству отдельных видов деятельности, различным образом связанных с кибербезопасностью, в т.ч. по международным принципам в области ИКТ, управление системами допуска, текущая диагностика систем, а также кибер-страхование.

Дженнифер МакАрдл (Jennifer McArdle) – научный сотрудник Центра революционной технической мысли Потомакского института политических исследований. Сфера научных интересов: кибер-войны, информационные войны и геополитика Азии. В настоящее время – кандидат на звание Доктор философии Кингз колледж, Лондон, отделение изучения войн и военного дела.

Франческа Спидальерис (Francesca Spidalieriis) - эксперт проекта Индекс кибер-готовности Потомакского института политических исследований. Также является старшим научным сотрудником по кибер-лидерству в Пелл-центре, университет Салве Регина. Сфера научных интересов: развитие кибер-лидерства, управление кибер-рисками, кибер-образование, а также обучение специалистов в области кибербезопасности. Недавно опубликовала отчет «Положение дел в кибербезопасности в штатах», содержащий оценки кибер-готовности разных штатов США в соответствии с данными ИКГ 1.0.

БИБЛИОГРАФИЯ

1. Индекс кибер-готовности 2.0 основывается на предыдущем Индексе кибер-готовности 1.0, который содержал методологию оценки стран по пяти категориям, в частности: национальная стратегия, реагирование на кризисы, киберпреступность и законодательство, обмен информацией, а также исследования и разработка. В рамках ИКГ 1.0 эта методология применялась в отношении 35 стран. Чтобы узнать больше об ИКГ 1.0, смотри: Melissa Hathaway, “Cyber Readiness Index 1.0,” Hathaway Global Strategies LLC (2013), http:// belfercenter. ksg.harvard.edu/files/ cyber-readiness-index-1point0.pdf.

2. Зависимость инфраструктуры от интернета заключается в зависимости основных критических услуг от наличия и качества интернет соединения (среди услуг в т.ч. и такие как водопровод, электроснабжение, транспорт, коммуникации, здравоохранение и т.п.). Чтобы узнать больше, см: Melissa Hathaway, “Connected Choices: How the Internet Is Challenging Sovereign Decisions,” American Foreign Policy Interests 36, no. 5 (November 2014): 301.

3. Примеры экономических стратегий на основе ИКТ: Единый европейский цифровой рынок, Цифровая единая Индия, Интернет-плюс (Китай), а также программа МСЭ ITU Connect 2020.

4. State Council of China, “Internet Plus,” Guo Fa 40 (2015). Translated by U.S. State Department.

5. Government of India, “Programme Pillars,” Digital India: Power to Empower, http://www.digitalindia. gov. in/content/programme-pillars.

6. European Commission, “Digital Single Market: Bringing down the barriers to unlock online opportunities,” http://ec.europa.eu/priorities/ digital-single-market/.

7. Melissa Hathaway and Francesca Spidalieri, “Sustainable and Secure Development: A Framework for Resilient Connected Societies,” in Observatory of Cyber Security in Latin America and the Caribbean (forthcoming December 2015 Organization of American States publication).

8. World Bank, “Overview,” Information & Communication Technologies Program, last modified 2 October 2014,http:// worldbank.org/en/ topic/ict/overview.

9. David Dean et al., “The Digital Manifesto: How Companies and Countries Can Win in the Digital Economy,” Boston Consulting Group report (January 2012): 2.

10. Peter C. Evans and Marco Annunziata, “Industrial Internet: Pushing the Boundaries of Minds and Machines,” General Electric (26 November 2012): 13.

11. Melissa Hathaway, “Cyber Readiness Index 2.0 & Lessons Learned in the Design of national Cyber Security Strategies,” (presentation at the OAS-IDB Regional Workshop on Cyber Security Policies, Washington D.C., 23 October 2014).

12. Frontier Economics London, Estimating the Global Economic and Social Impacts of Counterfeiting and Piracy: A Report commissioned by Business Action to Counterfeiting and Piracy, (London, Frontier Economics Ltd, 2011): 47.

13. The National Bureau of Asian Research, “The IP Commission Report: The report of the commission on the theft of American intellectual property,” National Bureau of Asian Research (May 2013).

14. Melissa Hathaway, “Connected Choices: How the Internet Is Challenging Sovereign Decisions,”

American Foreign Policy Interests 36, no. 5 (November 2014): 301.

15. Harvey Poppel is credited with inventing Harvey Balls in the 1970s while working at Booz Allen Hamilton as a consultant.

16. Based on 2013 World Bank GDP rankings.

17. OECD, OECD Digital Economy Outlook 2015 (Paris, France: OECD Publishing, 2015), http:// dx.doi. org/10.1787/9789264232440-en.

18. Melissa Hathaway, “Transparency, Trust, and Our Internet,” (presentation at GTEC Conference, Ottawa, Canada, 20 October 2015).

19. Развитие ИКТ инфраструктуры включает фиксированную и мобильную связь (голосовую и цифровую), по контрактам и подписке, а также инвестиции и доходы телекоммуникационного сектора экономики.

20. Компетентный орган – любое лицо или организация, имеющая законные полномочия или власть, возможности или ресурсы для реализации своей функции.

21. International Telecommunications Union, “National Strategies,” http:// www.itu.int/en/ITU-D/ Cybersecurity/ Pages/National-Strategies.aspx.

22. Термины КРКБ и ККР обозначают команды экспертов в области кибер-безопасности, обученные реагировать в случае инцидентов и кризисов. Оба термина могут быть взаимозаменяемыми, хотя КРКБ используется чаще.

23. The International Telecommunications Union, “CIRT Programme,” http:// www.itu.int/en/ITU-D/ Cybersecurity/ Pages/Organizational-Structures. aspx.

24. John Haller, Samuel Merrell, Matthew Butkovic, and Bradford Willke, Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability, Version 2.0 (Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2011), http://resources. sei.cmu.edu/ library/asset-view.cfm?AssetID=9999.

25. Olaf Kruidhof, “Evolution of National and Corporate CERTs – Trust, the Key Factor,” in Best Practices in Computer Network Defense: Incident Detection and Response, ed. Melissa E. Hathaway, (Amsterdam: NATO Science for Peace and Security Series, IOS Press, February 2014).

26. Singapore Computer Emergency Response Team, “FAQs,” https://www. csa.gov.sg/singcert/about-us/ faqs.

27. Ministério das Comunicações, “Portaria Interministerial N 147, de 31 de Maio de 1995,” http:// cgi.br/portarias/numero/147.

28. cert.br, “About CERT.br,” http:// www.cert.br/about/.

29. “Documents,” APCERT. APCERT. org, 13 October 2015. http://www. apcert.org/documents/index.html.

30. “Asia Pacific Computer Emergency Response Team Operational Framework” APCERT. APCERT. org, 13 October 2015. http://www.apcert.org/ documents/pdf/OPFW(26Mar2013).pdf.

31. Melissa Hathaway, “Best Practices in Computer Network Defense: Incident Detection and Response,” Global Cyber Security Center (September 2013): 12.

32. Ingvar Hellquist (Colonel retd.), Senior Advisor and Lars Nicander, Director, Center for Asymmetric Threat Studies, Swedish Defence University, “CATS Course and Cyber Exercise,” (interview by Melissa Hathaway in Stockholm, Sweden, 17 October 2012) and Swedish National Defence College, “CATS Newsletter,” CATS Center for Asymmetric Threat Studies (Spring 2013).

33. Dusan Navratil, Director Czech Republic National Security Authority and Robert Kahofer, Special Assistant, “Cyber Czech 2015 - National Technical Cyber Security Exercise,” (interview by Melissa Hathaway in Washington DC, October 2015).

34. “South Korea says Nuclear Worm is nothing to worry about,” TheRegister. co.uk, 30 December 2014, http://www. theregister.co.uk/2014/12/30/ south_korea_says_nuclear_worm_is_nothing_to_ worry_about/ and “Activists Hack KNHP’s computer systems,” World Nuclear News, 22 December 2014, http://www. world-nuclear-news.org/C-Activists-hackKHNPs-computer-systems-2212141. html.

35. Department of Homeland Security, “Cyber Storm: Securing Cyber Space,” http://www.dhs.gov/ cyber-storm-securing-cyber-space.

36. European Commission, “Cyber Strategy of the European Union: An Open, Safe, and Secure Cyberspace,” Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, (July 2013): 7 and European Union Agency for Network and Information Security, “Cyber Europe,” https://www. enisa.europa.eu/activities/Resilience-and-CIIP/ cyber-crisis-cooperation/ cce/cyber-europe.

37. Doug Drinkwater, “Hundreds of companies face two thousand cyber-attacks in EU exercise,” SC Magazine, 31 October 2014 in ENISA, “ENISA Cyber Europe 2014: Media Coverage,” https:// www.enisa.europa.eu/activities/ Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2014/ cyber-europe-2014-information/ cyber-europe-2014-media-coverage.

38. European Defense Agency, “Complex Cyber Crisis Management Exercise in Vienna,” 16 September 2015, https://www.eda.europa.eu/info-hub/ press-centre/latest-news/2015/09/16/ complex-cyber-crisis-management-exercise-in-vienna and NATO, “Largest ever NATO cyber defence exercise gets underway,” 21 November 2014, http://www.nato.int/cps/en/natohq/ news_114902. htm?selectedLocale=en.

39. Katie Bo Williams, “US, UK to test finance sector cybersecurity this month,” The Hill, 2 November 2015, http://thehill.com/policy/ cybersecurity/258827-us-uk-to-test-finance-sector-cybersecurity-this-month.

40. CNCERT/CC, “2nd China-Japan-Korea CSIRT Annual Meeting for Cybersecurity Incident Response was held in Korea,” www.cert.org.cn/ publish/englis h/55/2014/20140916145739295996084 /20140916145739295996084_.html.

41. Carnegie Mellon University, “List of National CSIRTs,” CERT Division, http:// www.cert.org/ incident-management/ national-csirts/national-csirts.cfm.

42. European Network and Information Security Agency (ENISA), “ENISA- CERT Inventory: Inventory of CERT teams and activities in Europe,” ENISA Version 2.16 (June 2014), http://www.enisa. europa. eu/activities/cert/background/inv/files/ inventory-of-cert-activities-in-europe.

43. Forum of Incident Response and Security Teams (FIRST), “FIRST Members,” http://www.first.org/ members/teams.

44. Council of Europe, Convention on Cybercrime (23 November 2001) and Shanghai Cooperation Organisation, Cooperation in the Field of Information Security, 61 plenary meeting (16 June 2009).

45. Там же.

46. Shanghai Cooperation Organisation, Cooperation in the Field of Information Security, 61 plenary meeting (16 June 2009), https://ccdcoe. org/ sites/default/files/documents/ SCO-090616-IISAgreementRussian.pdf.

47. Judge Stein Schjolberg and Amanda M. Hubbard, “Harmonizing National Legal Approaches on Cybercrime,” International Telecommunication Union (1 July 2005): 6.

48. Те двадцать стран, что подписали отчет Генассамблеи: Беларусь, Бразилия, Китай, Колумбия, Египет, Эстония, Франция, Германия, Гана, Израиль, Кения, Малайзия, Мексика, Пакистан, Республика Корея, Россия, Испания, Великобритания, США. Подробнее смотри: United Nations, Report of the Group of Government Experts On Development in the Field of Information and Telecommunications In the Context of International Security, A/65/201 and A/68/98 (26 June 2015).

49. Ernesto U. Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement, and Research (Dordrecht, The Netherlands: Springer, 2004): 50.

50. Advanced Centre for Research, Development and Training in Cyber Laws and Forensics, “Academic Programs,” National Law School of India University, https:// www.nls.ac.in/index.php?option=com_ cont ent&view=article&id=502&Itemid=32.

51. INTERPOL, “The INTERPOL Global Complex for Innovation,” accessed 17 September 2015, http://www.interpol. int/About-INTERPOL/ The-INTERPOL-Global-Complex-for-Innovation.

52. Madan M. Obero, “Dark Web and Crypto-Currency,” (presentation at Cyber 360: A Synergia Conclave, Bangalore, India, 30 September 2015).

53. Бот – вредоносное ПО, которое может использовать пользовательский компьютер для рассылки спама, размещения фишингового сайта, либо «кражи цифровой личности» методом отслеживания нажатия клавиш на клавиатуре. Инфицированные компьютеры контролируются третьей стороной и могут использоваться в качестве оружия в ходе кибер-атак. Чтобы узнать больше, смотри: Melissa Hathaway and John Savage, “Stewardship of Cyberspace: Duties of Internet Service Providers,” Cyber Dialogue 2012 (March 2012).

54. Alastair Stevenson, “Botnets infecting 18 systems per second, warns FBI,” V3.cok. uk, 16 July 2014, http://www.v3.co.uk/ v3-uk/news/2355596/ botnets-infecting18-systems-per-second-warns-fbi.

55. Bell Canada et all, “The Dark Space Project,” Security Telecommunications Advisory Committee (2011): 13, https://citizenlab.org/cybernorms2012/ cybersecurityfindings.pdf.

56. Yurie Ito, “Cyber Clean Center,” (remote interview with Cyber Readiness Index team, Washington DC, 10 November 2015).

57. Ministry of Internal Affairs and Communications and Ministry of Economy Trade and Industry, “What is the Cyber Clean Center,” Cyber Clean Center, https:// www.telecom-isac.jp/ccc/en_index. html and Michael M. Losavio, J. Eagle Shutt, and Deborah Wilson Keeling, “Changing the Game: Social and Justice Models for Enhanced Cyber Security,” in Tarek Saadawi, Louis H Jordan Jr., and Vincent Boudreau, Cyber Infrastructure Protection Volume II (U.S. Army War College, Strategic Studies, 2013): 101.

58. Telecom-ISAC Japan, “Chairman’s Message,” 12 May 2011, https://www. telecom-isac.jp/english/ index.html.

59. Australian Internet Security Initiative (AISI), “Overview of the Australian Internet Security Initiative,” http://www. acma.gov.au/Industry/ Internet/e-Security/ Australian-Internet-Security-Initiative/ australian-internet-security-initiative.

60. McAfee, “McAfee and CSIS: Stopping Cybercrime Can Positively Impact World Economies,” June 9, 2014, http://www.mcafee.com/us/about/ news/2014/q2/20140609-01.aspx and The National Bureau of Asian Research, IP Commission Report: The report of the commission on the theft of

American intellectual property," National Bureau of Asian Research (May 2013).

61. Melissa Hathaway, "Why Successful Partnerships are Critical for Promoting Cybersecurity," The New New Internet, 7 May 2010.

62. Netherlands Ministry of Security and Justice, "National Cyber Security Centre (NCSC)," https://www.ncsc.nl/english.

63. В феврале 2007 года Национальный центр координации сил безопасности объединился с Национальным консультационным центром в области безопасности, образовав Центр защиты национальных инфраструктур (CPNI). Чтобы узнать больше, смотри: Center for Protection of National Infrastructure, http://www.cpni.gov.uk.

64. Information-technology Promotion Agency (IPA), Japan IT Security Center, Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP) Annual Activity Report FY2012, (April 2013).

65. Financial Services-Information Sharing and Analysis Center, "Overview of the FS-ISAC," accessed 17 September 2015, https://www.fsisac.com/sites/default/files/ FS-ISAC_ Overview_2011_05_09.pdf.

66. National Cyber-Forensics & Training Alliance, "Become a NCFTA Partner," https://www.ncfta.net/become-ncft-partner.aspx.

67. Raphael Mandarino, "MT2: Private Public Partnership," Institucional Security Cabinet, Department of Information Security and Communications, Office of the President, (presentation at 1st INTERPOL Security Conference, Hong Kong, 15-17 September 2010).

68. National Institute for Standards and Technology, "National Vulnerability Database," https://nvd.nist.gov.

69. В Великобритании и Бразилии существуют механизмы де-классификации (публикации или предоставления партнерам) разведывательной или аналитической информации и предоставления ее критически важным предприятиям коммерческого сектора. Эта практика намного эффективнее, чем используемая в США.

70. European Commission, "ICT Research & Innovation," Horizon 2020: The EU Framework Programme for Research and Innovation, http://ec.europa.eu/programmes/horizon2020/ en/area/ict-research-innovation.

71. For more on the Networking and Information Technology Research and Development Program (NITRD) and its research areas, see: www.nitrd.gov/Index. aspx and NITRD, "The Networking and Information Technology and Research Development Program," Supplement to the President's Budget FY 2016

72. Consulate General of Israel in New York, "Cabinet approves tax break for National Cyber Park," Consulate General of Israel in New York, 7 June 2014, http://embassies.gov.il/wellington/NewsAndEvents/Pages/Cabinet-approves-tax-break-forNational-Cyber-Park-6-Jul-2014.aspx

73. Ciência Sem Fronteiras, "FAQ", http://www.cienciasemfronteiras.gov.br/web/csf-eng/faqEGTI_2013-2105_v1-3, Coordination for the Improvement of Higher Education Personnel (CAPES), "Coordination for the Improvement of Higher Education Personnel (CAPES)", http://www.iie.org/Programs/CAPES, and CNPq, "Programas Institucionais de Iniciação Científica e Tecnológica," http://www.cnpq.br/web/guest/piict

74. "Cyber Security," The Hague Security Delta, https://www.thehaguesecuritydelta.com/cyber-security

75. Zach Cutler, “5 Growing Cyber-Security Epicenters Around the World,” Entrepreneur, 3 September 2015, http://www.entrepreneur.com/article/250024.

76. European Commission, “About TTIP,” Trade, http://ec.europa.eu/trade/policy/in-focus/ttip/about-ttip/.

77. “Welcome to the U.S.-EU Safe Harbor,” http://www.export.gov/safeharbor/eu/eg_main_018365.asp.

78. Court of Justice of the European Union, “The Court of Justice declares that the Commission’s US Safe Harbour Decision is invalid,” Press Release 117/15 (6 October 2015), http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.

79. American Chamber of Commerce to the European Union, “EU Courts of Justice’s decision in the Schrems casecould disrupt transatlantic business, hurt the EU economy and jeapordise a Digital Single Market,” Press Release, 6 October 2015, http://www.amchameu.eu/sites/default/files/press_releases/press_-_ecj_decision_on_schrems_will_disrupt_transatlantic_business.pdf.

80. Hathaway, “Connected Choices: How the Internet Is Challenging Sovereign Decisions,” 302 and Arun Mohan Sukmar, “The New Great Game in Asia,” The Hindu, 25 August 2015, accessed September 16, 2015, http://www.thehindu.com/opinion/op-ed/arun-mohan-sukumar-column-the-newgreat-game-in-asia/article7575755.ece

81. “Wassenaar Arrangement on Export Controls for Conventional Arms and Dual Use Goods and Technologies” last updated 16 September 2015, http://www.wassenaar.org/index.html.

82. United Nations, Report of the Group of Government Experts On Development in the Field of Information and Telecommunications In the Context of International Security, A/65/201 and A/68/98 (26 June 2015).

83. The White House Office of the Press Secretary, “FACT SHEET: President Xi Jinping’s State Visit to the United States,” 25 September 2015, https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-presidentxi-jinpings-state-visit-united-states

84. University of Toronto, “VII: BRICS Summit 2015 Ufa Declaration,” BRICS Information Centre, 9 July 2015, http://www.brics.utoronto.ca/docs/150709-ufa-declaration_en.html.

85. United Nations, General Assembly, “Letter dated 9 January 2015 from Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General,” Developments in the field of information and telecommunications in the context of international security, A/69/723 (13 January 2015), http://daccess-dds-ny. un.org/doc/UNDOC/GEN/N15/014/02/ PDF/N1501402.pdf?OpenElement.

86. Melissa Hathaway, “Discussion Paper for the Global Commission of Internet Governance,” (paper presented in Stockholm Sweden, 27 May 2014).

87. Inter-American Development Bank, “IDB and OAS join efforts to promote better cybersecurity policies in Latin America and the Caribbean,” 22 October 2014, http://www.iadb.org/en/news/ news-releases/2014-10-22/cybersecurity-workshop-for-latin-america,10957.html.

88. Dusan Navratil, Director Czech Republic National Security Authority and Robert Kahofer, Special Assistant, “Cyber Czech 2015 - National Technical Cyber Security Exercise,” (interview by Melissa Hathaway in Washington DC, October 2015) and Rueuven Azar, Deputy Chief of Mission and Dr. Eviatar Matania, Head of National Cyber Bureau (interview by Melissa Hathaway in Rockville, MD, 2 June 2015).

89. Craig L. Hall, US Consulate General, Kolkata, India, (interview by Melissa Hathaway in Kolkata, India, 23 September 2015).

90. Кибер-конфликт отличается от кибер-войны или кибер-сражения. Последнее – чрезвычайно технологичное событие и, в принципе, может происходить полностью и исключительно в сети, не выходя в реальный мир. Сражение обычно является компонентом войны или конфликта. «Кибер-конфликты – важные для стран агрессивные и разрушительные конфликты, для которых результаты, которыми они заканчиваются, не имели бы места без «кибер» (т.е. сетевых компьютерных технологий) механизмов в качестве важнейшего связующего звена в цепи происходящих событий». Chris Demchak, “Resilience, Disruption, and a ‘Cyber Westphalia’: Options for National Security in a Cybered Conflict World,” in Securing Cyberspace: A New Domain for National Security, edited by Nicholas Burns and Jonathon Price, (Washington, DC: The Aspen Institute, 2012).

91. Christopher Bronk, “The Cyber Attack on Saudi Aramco,” Survival 55 (April-May 2013) 81-96.

92. Melissa Hathaway and John Stuart, “Cyber IV Feature: Taking Control of our Cyber Future,” Georgetown Journal of International Affairs (25 July 2014).

93. Robert M. Lee, Michael J. Assante, and Tim Conway, “German Steel Mill Cyber Attack,” Industrial Control Systems (30 December 2014).

94. “The Reality of the Sony Pictures Breach,” TrendMicro, 22 December 2014, http://blog. trendmicro.com/reality-sony-pictures-breach/, Sean Fitz-Gerald, “Everything That’s Happened in the Sony Leak Scandal,” Vulture, 22 December 2014, http://www.vulture. com/2014/12/everything-sony-leaks-scandal.html#, and “Sony Breach May Have Exposed Employee Healthcare, Salary Data,” Krebson Security, 2 December 2014, http:// krebsonsecurity. com/2014/12/sony-breach-may-have-exposed-employee-healthcare-salary-data/.

95. Jennifer Valentino-Devries and Danny Yadron, “Cataloging the World’s Cyberforces,” The Wall Street Journal, 11 October 2015, http:// www.wsj.com/ articles/cataloging-the-worlds-cyberforces-1444610710 and United Nations, General Assembly, Developments in the Field of Information and Telecommunications in the context of International Security: Report to the Secretary General, A/70/172 (22 July 2015), http://www. un.org/ga/search/ view_doc.asp?symbol=A/70/172.

96. James Lewis and Katrina Timlin, “Cybersecurity and Cyberwarfare 2011: Preliminary Assessment of National Doctrine and Organization,” UNIDIR Resource and Center for Strategic and International Studies (2011): 3.

97. Department of Defense, “The Department of Defense Cyber Strategy,” (April 2015): 7-8.

98. President of the Russian Federation, “Military Doctrine of the Russian Federation,” Russian Government (2014) translated by Thomas Moore, https:// www.scribd.com/doc/251695098/ Russia-s-2014-Military-Doctrine.

99. Ministry of Defense of the Russian Federation, “Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space,” (2011) translated by the US Department of State.

100. “The new doctrine of information security pointed out the danger of destabilization via the Internet,” Russian News, 10 September 2015, http:// en.news-4-u. ru/the-new-doctrine-of-information-security-pointed-out-the-danger-of-destabilization-via-the-internet.html.

101. Министерство обороны Бразилии также недавно дало указание Совместному комитету командующих Вооруженными силами упрочить национальную кибер-оборону посредством

создания трехсторонней Команды кибер-обороны (ComDCiber). Несмотря на то, что ComDCiber объединит специалистов из всех трех организаций, армия будет являться ведущей в этом органе. ComDCiber будет расположен в ранее созданном Бразильском центре уибер-обороны Нуклеус (NU CDCiber) в столице, городе Бразилиа. Чтобы узнать больше, смотри: EeInigo Guevara, “Brazil to stand up Cyber Defence Command,” IHS Jane’s Defence Weekly, 4 November 2014 and Diego Rafael Canabarro and Thiago Borne, “Brazil and the Fog of (Cyber) War,” National Center for Digital Governance (2013): 5. On Korea’s cyber capabilities, see : Republic of Korea, “Defense White Paper,” (2014), 57, http:// www.mnd.go.kr/user/mnd_eng/upload/pblictn/ PBLICTNEBOOK_201506161156164570.pdf.

102. Zachary Keck, “South Korea Seeks Offensive Cyber Capabilities,” The Diplomat, October 11, 2014, http:// thediplomat.com/2014/10/ south-korea-seeks-offensive-cyber-capabilites/.

103. For an overview of China’s cyber strategy, see: Amy Chang, “Warring States,” The Center for New American Security, (December 2014).

104. Information Office of the State, “White Paper: The Diversified Employmenet of China’s Armed Forces,” April 2013, http://eng.mod.gov.cn/ Database/ WhitePapers/ and Xi Jinping, Cental Military Commission, “Opinion on Further Strengthening Military Information Security Work,” partial translation from Amy Chang, “Warring States,” The Center for New American Security, (December 2014): 20.

105. Director Generals of Nordic Council, “Icelandic Cyber Responsibilities,” (meeting between Melissa Hathaway and Director Generals and respective delegations of the Nordic Council who are responsible for National Computer Emergency Response Teams, Stockholm, Sweden, 19 November 2014).

106. Minister of the Interior, “Icelandic National Cyber Security Strategy 2015-2026: Plan of Action,” Icelandic Minister of the Interior (June 2015), http:// eng.innanrikisraduneyti.is/media/ frettir-2015/ Icelandic_National_Cyber_Security_Summary_ loka.pdf.

107. Yaakov Katz, “Security and Defense,” The Jerusalem Post, 8 October 2010 in James Lewis and Katrina Timlin, “Cybersecurity and Cyberwarfare 2011: Preliminary Assessment of National Doctrine and Organization,” UNIDIR Resource and Center for Strategic and International Studies (2011), 14 and “Eye on tech exports, Israel launches cyber command,” Reuters, 18 May 2011, http://www.reuters.com/ article/2011/05/18/us-israel-security-cyber-idUSTRE74H27H20110518.

108. Mitch Ginsburg, “Army to establish unified cyber corps,” The Times of Israel, June 16, 2015.

109. Michael Herzog, “New IDF Strategy Goes Public,” The Washington Institute: Policy Watch 2479 (28 August 2015), http://www.washingtoninstitute.org/ policy-analysis/view/ new-idf-strategy-goes-public.

POTOMAC INSTITUTE FOR POLICY STUDIES
901 N. Stuart St. Suite 1200, Arlington, VA 22203
www.potomacinstitute.org