Как справляться с национальными киберрисками?

Мелисса Хэтэуей (Melissa Hathaway)

Введение

За последние 30 лет государства, хозяйствующие субъекты и граждане стали критически зависимыми от Интернета и информационно-коммуникационных технологий (ИКТ). Мы рассчитываем на бесперебойность функционирования жизненно важных систем электропитания и связи, уверены в том, что товары, услуги, данные и капитал будут беспрепятственно пересекать границы. При этом многие сетевые системы и инфраструктуры оказываются очень уязвимыми, чем умело пользуются недоброжелатели. Разные организации все чаще сталкиваются с кражей данных, становятся жертвами киберпреступников, испытывают нарушения обслуживания, теряют имущество. В целом растет общее ощущение незащищенности. Более 100 стран и быстро растущее число негосударственных субъектов и отдельных лиц способны наносить ущерб государственным и хозяйственным сетевым инфраструктурам. Каждый субъект киберпреступности преследует свои цели – от политических до мошенничества и других видов преступности с применением ИКТ; от кражи интеллектуальной собственности (ИС) до шпионажа; от атак на отказ в обслуживании до уничтожения материальных активов и другого имущества. Государства, хозяйствующие субъекты и отдельные физические лица постоянно находятся в условиях *отсутствия информационной безопасности (кибербезопасности)* перед лицом множества киберрисков, что выводит на первый план необходимость, в известной степени, коллективного разделения ответственности за управление ими. Последние события убедительно указывают на необходимость выработки общего дисциплинированного подхода к управлению рисками в сфере ИКТ и его включения в стратегии (концепции) информационной безопасности и цифровые повестки дня. Бездействие в этой сфере смерти подобно.

Риск определяется с точки зрения времени – когда кто-то (что-то) подвержен (-о) опасности или вероятности нанесения ущерба (причинения убытков).[1] Условия риска могут изменяться в зависимости от действий, предпринимаемых по меньшей мере двумя участниками этих отношений – злоумышленником, который завладевает силами и средствами причинения вреда и применяет их, и предполагаемым объектом нападения, который может принять меры предосторожности в целях противодействия злоумышленнику или срыва его планов. Каждый день наша цифровая зависимость растет, но понимание рисков, связанных с этой зависимостью, остается на зачаточном уровне. Тем не менее, риски в сфере ИКТ продолжают расти на фоне широкого спроса на доступные – по наличию и цене – вредоносные программы и сервисы, незаконные услуги и конфиденциальные (непубличные) данные. Например, вредоносное программное обеспечение можно приобрести всего за один доллар, а проведение распределенной атаки типа «отказ в обслуживании» обойдется в сумму, не превышающую тысячу долларов. Сложные атаки в целях вымогательства выкупа (ransomware attacks) доступны в пределах

двухсот долларов, а вредоносные сервисы электронной почты с распространением спама доступны примерно за четыреста долларов.[2] Можно найти в Сети и скачать даже самые изощренные программные решения боевого назначения, применяемые государственными спецслужбами.[3] Доступ к этим средствам открыт любому, кто захочет их использовать для проведения атак и причинения вреда. Как показывают события 2017 года, от некоторых из известных кибератак пострадали государства, компании и люди.

Так, в мае 2017 года злоумышленники воспользовались недочетами в операционных системах Microsoft Windows и провели атаки в целях вымогательства выкупа на миллионы компьютеров в 150 странах в разных отраслях экономики. В результате применения очень простой вредоносной программы WannaCry в глобальных масштабах были остановлено проведение производственных операций, функционирование транспортных и телекоммуникационных систем. По данным Национального контрольно-ревизионного управления Великобритании, атаки с помощью программы WannaCry вызвали перебои в работе по меньшей мере 81 из 236 объектов национальной системы здравоохранения страны и выход их строя медицинского оборудования, что существенно сказалось на общественном здравоохранении и безопасности.[4]

В июне 2017 года в Сеть была запущена новая вредоносная программа еще более разрушительной силы – NotPetya. Она была запущена под видом механизма обновления популярной бухгалтерской программы (doc.me). В течение нескольких минут вредоносная программа заразила десятки тысяч подключенных к Интернету систем, в том числе принадлежащих государственным учреждениям, банкам, энергетическим и другим компаниям, в более чем 65 странах. Например, атака с помощью вируса NotPetya на крупнейшую в мире морскую транспортную компанию A.P. Moller-Maersk привела к зашифровке и уничтожению ее информационно-коммуникационных систем во всем мире. Вследствие этого компании пришлось остановить операции на большей части из числа 76 портовых терминалов по всему миру, что привело к срыву морских торговых перевозок в течение нескольких недель. Финансовые потери Maersk вследствие атаки NotPetya превысили 300 миллионов долларов, так как компании пришлось перестроить всю свою инфраструктуру, включая установку 4000 новых серверов, 45 тысяч новых компьютеров и 2500 новых приложений.[5] По некоторым оценкам, во всем мире атака NotPetya причинила убытки в миллиарды долларов из-за срывов бизнес-операций и разрушения материального имущества.[6] Потери первичного и побочного характера, понесенные цифровой экономикой, были весьма значительными, и потребовались месяцы для устранения нанесенного ущерба и восстановления функционирования критически важных сервисов (оказания услуг) и объектов инфраструктуры.

Еще более тревожным событием стала внезапная вынужденная остановка одного нефтегазового объекта на территории Саудовской Аравии в августе 2017 года в результате воздействия вредоносной программы Trisis – компьютерного вируса, специально

предназначенного для выведения из строя промышленных систем управления (ПСУ). Это вредоносное программное обеспечение боевого класса предназначено для целевого воздействия на оперативные компоненты ИКТ, используемых на объектах топливно-энергетического комплекса и систем водоснабжения, а также на физические механизмы безопасности (системы аварийного отключения) ПСУ. Хотя это всего лишь один известный пример успешного использования этого разрушительного программного обеспечения, компания Schneider Electric предупредила своих клиентов и владельцев инфраструктур о необходимости обеспечения их диверсификации и резервирования на случай возможных подобных отказов в будущем вследствие аналогичных атак.[7]

Произошедшие в 2017 году инциденты в сфере ИКТ демонстрируют крайнюю пагубность кибератак, при этом использованные киберпреступниками инструменты не отличались особой изощренностью. За последние пять лет число целевых атак на объекты ТЭК, телекоммуникационные системы, транспорт и финансовые системы почти удвоилось, что представляет общую угрозу для экономики и национальной безопасности. Все это указывает на настоятельную необходимость объединения усилий государственных структур и хозяйствующих субъектов в целях активизации и повышения эффективности процессов управления рисками в сфере ИКТ и их всеобъемлющего учета в документах стратегического планирования.

Механизмы оценки, предупреждения и ликвидации последствий рисков в сфере ИКТ

Страны, международные организации и научные учреждения разрабатывают рамочные механизмы, призванные содействовать предупреждению и снижению рисков в сфере ИКТ в интересах руководителей государств и хозяйствующих субъектов. Необходимость в таких механизмам обусловлена тем, что в течение последних трех десятилетий эти руководители пользовались преимуществами информационных технологий для обеспечения роста производительности, повышения эффективности, снижения капитальных затрат, хранения и обработки данных – все в интересах экономического развития, но при этом не торопились с инвестициями в безопасность и отказоустойчивость своих сетевых инфраструктур, обслуживающих цифровую экономику. Активная разрушительная деятельность злоумышленников в сфере ИКТ требует от руководства стран и корпораций принятия неотложных мер, направленных на обеспечение безопасности киберпространства в интересах всего общества. При этом потери накапливаются, ущерб растет, опасность становится неминуемой.

Государственные механизмы

Государства начали разрабатывать механизмы, контрольные ориентиры и комплексные национальные концепции информационной безопасности на основе формирования более глубокого понимания их растущей зависимости от ИКТ и анализа уязвимых мест в целях

обеспечения безопасности общенациональных сетей, инфраструктур и сервисов, от которых зависит их цифровое будущее и экономическое благополучие. Однако, когда дело доходит до выявления и устранения рисков в сфере ИКТ той или иной страны, по-прежнему остается открытым вопрос: как можно предупредить и уменьшить риск, который наступил уже более 30 лет назад?[8] Важно начать с понимания того, что представляет собой стратегический план страны на 3-5 лет, и определиться с тем, что можно сделать для достижения поставленных целей в долгосрочной перспективе. Например, в Нидерландах подсчитали, что к 2020 году не менее 25 процентов валового внутреннего продукта страны будет состоять из цифровой экономики (т.е. цифровых товаров и услуг). Установив, что их будущее зависит от способности обеспечить безопасность цифровой экономики, голландцы стали в известной степени выделять на это необходимые инвестиции и проводить структурные реформы. В других странах – в США и Германии – ведется отбор топ-компаний, создающих более 2 процентов ВВП страны, с тем чтобы совместными усилиями гарантировать учет задач по управлению рисками и обеспечению живучести (отказоустойчивости) в их всеобъемлющих планах развития и бизнес-процессах. Тем не менее, в большинстве стран принят более широкий подход, предусматривающий защиту «критически важных объектов инфраструктуры» – т.е. тех основных активов, систем и сетей, которые, как считается, становятся особенно уязвимыми вследствие растущей взаимной интегрированности и зависимости от Интернета, что делает их подверженными отказам техники, человеческому фактору, погодным условиям и другим природным причинам сбоев, а также атакам – физическим и с применением ИКТ.[9] Недостатком такого подхода является то, что он не предусматривает четкого разграничения ответственности между государством и хозяйствующими субъектами, а это затрудняет привлечение к ответственности виновных за бездействие. А тем временем дефицит безопасности всего общества все увеличивается на фоне отсутствия приверженности делу снижения рисков и повышения отказоустойчивости.

Некоторые государства решили усилить свою регулирующую функцию в экономике и потребовали от ряда отраслей выявления, оценки и устранения недостатков в их системах безопасности. Под требования регулятора попали следующие отрасли: электроэнергетика, финансы и банки, здравоохранение, транспорт и телекоммуникации. Меры регулирования также предусматривают обязательное подробное уведомление местных, региональных или национальных властей о фактах произошедших инцидентов в сфере ИКТ и категории взломанных (утерянных) данных, о методах взлома, а также о возможных сбоях в работе предприятий (телекоммуникаций).

Европейский союз устанавливает обязательность этих предписывающих подходов в отношении операторов критических инфраструктур и поставщиков жизненно важных услуг. В августе 2016 года ЕС принял «Директиву о сетях и информационной безопасности», которая установила требования обеспечения кибербезопасности в отношении поставщиков услуг, классифицируемых как «существенные». К таким услугам

отнесены следующие: энергетика, транспорт, банковское дело, финансы, водоснабжение и здравоохранение, а также цифровые – платформы электронной торговли (например, eBay, Amazon); поисковые системы (например, Google) и сервисы на основе облачных вычислений. Государства-члены ЕС обязаны до мая 2018 года привести свои национальные законодательства в соответствие с положениями данной Директивы, которая требует от поставщиков критически важных услуг в этих странах предпринять соответствующие меры безопасности и уведомлять соответствующие национальные компетентные органы или [созданные для этих целей] группы реагирования на инциденты, связанные с компьютерной безопасностью (CSIRT) о любых серьезных инцидентах. Таким образом укрепляется подотчетность и снижаются киберриски, поскольку операторы критически важных объектов инфраструктуры и поставщики жизненно важных услуг вынуждены принимать меры для снижения уязвимости и повышения устойчивости.

По аналогичному пути пошел и Китай, который даже включил отдельные положения Директивы ЕС в свой новый национальный закон «О кибербезопасности», принятый парламентом Китая в ноябре 2016 года и вступивший в силу 31 декабря 2017 года. Этот закон, содержащий семь глав и 79 статей, является «всеобъемлющим и всеохватывающим», поскольку определяет ответственность профильных государственных учреждений, поставщиков интернет-услуг и пользователей сети «Интернет». Согласно этому закону, хозяйствующие субъекты (организации, общества) – в широком понимании – должны принимать технические и другие необходимые меры для обеспечения безопасного и устойчивого функционирования Интернета, эффективного устранения инцидентов в сфере ИКТ, предотвращения преступной деятельности в сфере ИКТ и поддержания целостности, скрытности и доступности (пригодности для использования) интернет-данных.[10] Законодатель обязал компании вкладывать средства во внедрение новых механизмов защиты и управления в целях выполнения принципов информационной безопасности. Законом также предусматривается режим проверок и контроля для обеспечения того, чтобы компании проводили соответствующие мероприятия по снижению рисков и привлекались к ответственности в случае выявления недостаточности принимаемых мер в сфере кибербезопасности.

США воздержались от принятия регулирующего подхода и вместо этого призвали операторов критических инфраструктурных объектов страны и поставщиков жизненно важных услуг принимать меры по снижению рисков в сфере ИКТ на добровольной основе. В феврале 2013 года президент обратился к Национальному институту стандартов и технологий (NIST) с требованием разработать комплекс единых стандартов, методик, процедур и процессов, регулирующих нормативные, хозяйственные и технологические аспекты кибербезопасности. Годом позже, в феврале 2014 года, были опубликованы «Основы укрепления кибербезопасности жизненно важных инфраструктурных систем» («Framework for Improving Critical Infrastructure Cybersecurity»), содержащие комплекс добровольных нормативов по оценке рисков в сфере ИКТ, управлению ими и

реагированию на них. Согласно этому документу, организации должны производить оценку рисков по пяти категориям – выявление, защита, обнаружение, реагирование и восстановление (ликвидация последствий). По некоторым оценкам, Основами практически руководствуются в США примерно 30 процентов организаций (включая госструктуры) для оценки рисков несанкционированного доступа, нанесения ущерба или разрушения и повышения своей ответственности за защиту своих сетей и сохранение конфиденциальности данных.[11] Кроме того, в приложении к этому документу проводится привязка различных международных стандартов к категориям снижения риска в сфере кибербезопасности, принятым в NIST. Однако опыт недавних инцидентов показывает, что организации, использующие механизмы кибербезопасности по методике NIST, применяют установленные Институтом категории оценки рисков, скорее, для формального выполнения предъявляемых требований, а не в целях обеспечения постоянной оценки риска на регулярной основе. Так, некоторые организации, применив методику NIST, высоко оценили свой уровень кибербезопасности, но при этом впоследствии все равно значительно пострадали от атак с применением WannaCry и NotPetya.[12]

В сентябре 2017 года NIST опубликовал измененную и дополненную версию «Свода общих принципов управления рисками для информационных систем и организаций: системный подход жизненного цикла для обеспечения безопасности и конфиденциальности».[13] В «Своде…» устанавливается рекомендуемый порядок выявления организациями высокоценных активов и систем стратегического значения в своей структуре и оценки связанных с ними рисков. Устанавливается также рекомендуемый порядок определения и отбора средств контроля безопасности и защищенности информации, а также внедрения и оценки эффективности управления информационной безопасностью. При этом подчеркивается важность непрерывного мониторинга рисков в режиме реального времени вместо разнесенных в времени точечных мероприятий по выполнению требований безопасности в сфере ИКТ. В документе также указывается на необходимость включения в хозяйственнее решения мер по управлению рисками. «Свод …» служит дополнением к «Основам укрепления кибербезопасности жизненно важных инфраструктурных систем», и оба документа в совокупности служат организациям источником более стратегического подхода к проблеме управления рисками.

Международные механизмы

Международные организации также участвуют в обсуждении актуальных проблем управлениям рисками в сфере ИКТ и содействуют повышению оперативности принятия эффективных мер в области кибербезопасности на основе собственных механизмов и рекомендаций. Обсуждение актуальных проблем управления рисками обрело международные масштабы по итогам двух последовательных этапов (2003 и 2005 гг.) Всемирного саммита по вопросам информационного общества – глобального объединения сообществ «ИКТ для развития». Тогда по меньшей мере 170 стран решили объединить свои усилия в интересах взаимовыгодного использования возможностей, предоставляемых

ИКТ, путем улучшения доступа к информационно-коммуникационным технологиям, инфраструктуре, информации и знаниям; повышения доверия и безопасности в сфере ИКТ; развития и расширения применения ИКТ; а также содействия международному и региональному сотрудничеству.[14] С тех пор международные институты разрабатывают и распространяют рамочные механизмы управления рисками с учетом уязвимостей ИКТ, повышают уровень доверия к глобальной цифровой экономике и участия в ней.

Одной из первых международных организаций, взявшихся за это дело, была Организация американских государств (ОАГ). С 2004 года ОАГ через Межамериканский комитет по борьбе с терроризмом и его Программу кибербезопасности активно продвигает проблематику кибербезопасности на американском континенте. ОАГ сотрудничает с широким кругом организаций государственного и частного секторов на национальном и региональном уровнях по нормативно-регуляторным и техническим вопросам, преследуя цели создания и укрепления потенциала кибербезопасности в государствах-членах Организации посредством оказания технического содействия, организации обучения кадров, проведения круглых столов по вопросам нормативного регулирования, учений с отработкой вопросов антикризисного управления, а также обмена передовым опытом в сфере ИКТ. При этом ОАГ опирается на существующие государственные и научно-учебные механизмы для содействия наращиванию потенциала в области кибербезопасности и формирования в государствах-членах признания важности обеспечения безопасности киберпространства и инфраструктуры, которая его поддерживает. Если страны не будут в равной степени вкладываться в безопасность своих ключевых инфраструктур и обеспечение живучести своих систем, то ущерб, наносимый субъектами вредоносной деятельности в сфере ИКТ, будет тормозить экономический рост в этих странах.

В 2007 году Международный союз электросвязи (МСЭ) – специализированное учреждение ООН, отвечающее за сферу ИКТ, – объявил о своей Глобальной программе кибербезопасности (ГПК) и предложил механизм для содействия многостороннему сотрудничеству. ГПК основывается на пяти принципах, которыми должны руководствоваться страны при создании потенциала для обеспечения ответственного поведения в киберпространстве. К ним относятся: (1) меры по совершенствованию правовой базы; (2) меры технического и процедурного характера; (3) организационные структуры; (4) наращивание потенциала и (5) международное сотрудничество. В рамках этой инициативы в 2011 году было разработано Руководство по кибербезопасности МСЭ, в котором подчеркивается необходимость учета культурно-исторических особенностей и интересов каждой страны при разработке действенной стратегии информационной безопасности. В нем также освещаются важные вопросы, которые должно решать каждое государство при выводе проблематики кибербезопасности из рамок простой технической дискуссии на стратегический уровень национальной политики. На этой основе в 2014 году МСЭ запустил Глобальный индекс кибербезопасности (ГИК) как методику сравнительной

оценки состояния кибербезопасности стран и расчета необходимых инвестиций в этом направлении. Этот показатель предназначен для оценки состояния страны по пяти категориям ГПК – по совершенствованию правовой базы, по технике, организационным мерам, наращиванию потенциала и сотрудничеству.[15] Эта методика и индекс стали одними из первых международных инструментов, предоставленных странам для научного обоснования своих стратегий развития и обеспечения нетехнического подхода к измерению киберрисков.

В 2015 году Совет Организации экономического сотрудничества и развития (ОЭСР) принял и опубликовал «Рекомендации ОЭСР по управлению рисками в сфере цифровой безопасности для общественно-экономического процветания»,[16] которые предлагалось учитывать при разработке национальных стратегий, нацеленных на управление цифровой безопасностью и оптимизацию социально-экономических выгод от цифровой открытости. Странам рекомендовалось управлять рисками в сфере ИКТ на основе восьми взаимосвязанных, взаимозависимых и взаимодополняющих принципов высокого уровня, включая: (1) повышение осведомленности, приобретение навыков и расширение прав и возможностей; (2) ответственность заинтересованных сторон; (3) права человека и фундаментальные ценности; (4) сотрудничество; (5) цикл оценки и обработки рисков; (6) меры безопасности, соответствующие имеющимся рискам в отношении проводимой социально-экономической деятельности и соизмеримые с ними; (7) инновации и (8) планирование готовности и непрерывности. По мнению ОЭСР, при реализации этих восьми принципов в сочетании с другими международными механизмами странам удастся усовершенствовать свою политику (и стратегию) на основе передовых методик управления рисками в сфере цифровой безопасности. Не являясь собственно механизмом как таковым, указанные восемь принципов могут служить ключевыми компонентами процесса создания или усиления механизмов согласования усилий как внутри государственных структур, так и в отношениях с негосударственными заинтересованными сторонами. ОЭСР придает важное значение сотрудничеству государственного и частного секторов для снижения рисков в сфере ИКТ.

В 2018 году Всемирный экономический форум (ВЭФ) опубликовал «Наставление по сотрудничеству между государственным и частным секторами в интересах устойчивости к угрозам в сфере ИКТ» [17] – методика внутригосударственного государственно-частного сотрудничества в интересах кибербезопасности. В частности, в разделе 4.7 «Наставления…» обосновывается необходимость создания четкого национального механизма управления кибербезопасностью, включая функции, обязанности и возможности государственного и частного секторов. Предложенный ВЭФ трехъярусный механизм предоставляет государствам возможность распределить обязанности среди заинтересованных сторон с учетом трех аспектов безопасности – надежности, отказоустойчивости и защиты – при взаимном дополнении и укреплении друг друга. Надежность определяется как «способность предотвращать, отражать и сдерживать угрозы». Отказоустойчивость – как «способность управлять несанкционированными

взломами и ликвидировать их последствия». Наконец, защита определяется как «способность упреждать, срывать атаки и реагировать на них»."[18] Этот механизм основывается на инициативах, выдвинутых в 2014 году Советом Всемирной программы ВЭФ «О рисках и устойчивости», и Стратегии 2016 года «Понимание системных рисков в сфере кибербезопасности». В обсуждении киберрисков ВЭФ продвинулся к пониманию прямой связи между кибербезопасностью и экономикой.

Механизмы научных и экспертно-технических сообществ

Растет значимость научно-исследовательских учреждений, аналитических центров и экспертного сообщества, которые разработали различные методологии для повышения уровня готовности и зрелости стран и организаций.

Индекс готовности в сфере кибербезопасности 2.0 (CRI 2.0), [19] опубликованный в 2015 году группой экспертов Института политических исследований Потомака, основан на первой версии аналогичного индекса 2013 года, который позволил замерить степень т.н. киберготовности стран. Версия CRI 2.0 предоставляет собой всеобъемлющую сравнительную, основанную на практическом опыте методологию оценки приверженности и зрелости стран для устранения разрыва между их нынешним положением в области кибербезопасности и стратегическими установками на обеспечение их цифрового будущего. В методике CRI 2.0 используется более семидесяти уникальных показателей по семи основным элементам для выявления проводимых мероприятий в сфере готовности и выявления направлений дальнейшего совершенствования в следующих категориях: (1) национальная стратегия; (2) реагирование не инциденты; (3) электронная преступность и правоохранительная деятельность; (4) обмен информацией; (5) инвестиции в НИОКР; (6) дипломатия и торговля и (7) защита, антикризисное управление и ликвидация последствий кризисов. В результате вырабатывается план практических действий по снижению рисков, которому следуют страны. Самое главное, что CRI 2.0 связывает экономический рост и развитие с политикой в сфере национальной безопасности. Он также признает, что реализация *полного* потенциала интернет-экономики с точки зрения роста ВВП, повышение производительности и эффективности, повышение квалификации рабочей силы и улучшение доступа к бизнесу и информации – все это требует согласования стратегий экономического развития с приоритетами национальной безопасности. Иными словами, ИКТ могут обеспечить экономический рост только в случае установления нормативных мер, процессов и технологий, необходимых для обеспечения безопасности информационной инфраструктуры и сервисов, от которых зависит цифровое будущее и рост страны. CRI 2.0 позволяет выявить те инструменты, которые можно использовать для защиты инвестиций в цифровую экономику и устранения продолжающейся эрозии экономики от дефицита кибербезопасности. Такие инструменты лежат, в частности, в сфере государственного регулирования, нормативных требований, законодательства, стандартов, стимулирования рынка и др.

Модель зрелости потенциала кибербезопасности, опубликованная в 2016 году Центром изучения глобального потенциала кибербезопасности при Оксфордском университете, описывает различные уровни зрелости стран в сфере кибербезопасности с учетом пяти измерений потенциала кибербезопасности: (1) нормативное регулирование и стратегия в области кибербезопасности; (2) киберкультура и общество; (3) кибербезопасность, образование, обучение и навыки; (4) нормативно-правовая база и (5) стандарты, организации и технологии. Каждое из этих измерений разбивается далее на более конкретные коэффициенты и показатели, которые в совокупности отражают степень зрелости потенциала изучаемой страны в сфере кибербезопасности. В основе этой модели – два метода диагностики киберготовности. Первый метод основан на анкетировании (аналогично методике МСЭ), при котором государство самостоятельно диагностировать свою готовность. Затем ответы респондентов обобщаются и представляются для анализа по пяти категориям киберзрелости – начальный, формирующийся, установленный, стратегический и динамичный – в рамках семинара по техническому обмену с участием ключевых заинтересованных сторон от государства, науки, частного и государственного секторов. Оксфордская модель является отличным инструментом измерения уровня понимания со стороны ключевых заинтересованных сторон текущего состояния кибернетического потенциала и зрелости той или иной страны, что затем обеспечивает основу для формирования целей нормативной политики в области снижения киберрисков.

Наконец, на Таллиннской конференции об электронном государстве в мае 2016 года Академия электронного государства Эстонии предложила Национальный индекс кибербезопасности (NCSI), который в январе 2018 года был обновлен и модифицирован.[20] Эта методика выработана с учетом опыта Эстонии как одной из первых стран установившей электронное управление в масштабах всего общества. Версия NCSI 2.0 включает в себя двенадцать направлений оценки потенциала и 46 показателей, позволяющих оценить, на общенациональном уровне, способность страны создавать «безопасную» систему электронного государственного управления с защитой данных и транзакций при одновременном снижении цифровых рисков и подверженности им. Эти двенадцать направлений оценки потенциала включают следующие области: (1) способность разрабатывать национальные нормативные требования в области кибербезопасности; (2) способность анализировать киберугрозы на национальном уровне; (3) способность обеспечивать образование в области кибербезопасности; (4) способность обеспечивать базовую кибербезопасность; (5) способность обеспечивать безопасную среду для электронных услуг; (6) способность обеспечивать электронную идентификацию и электронные подписи; (7) способность защищать критическую информационную инфраструктуру; (8) способность к круглосуточному обнаружению киберинцидентов и реагированию на них; (9) способность управлять страной в условиях крупномасштабного кризиса в сфере ИКТ; (10) способность бороться с киберпреступностью; (11) способность проводить военные операции в области кибербезопасности и (12) способность обеспечивать международную кибербезопасность. При наличии множества компонентов, схожих с компонентами других [рассмотренных выше] механизмов, NCSI имеет ряд

уникальных особенностей, обусловленных опытом этой страны в области электронного государственного управления, в том числе в области создания безопасной среды для электронных услуг и обеспечения электронной идентификации и электронной подписи.

Краткие выводы по механизмам

У каждого механизма укрепления кибербезопасности и повышения эффективности управления рисками в сфере ИКТ на национальном уровне имеются свои особенности. При этом всем механизмам свойственно множество общих черт, в том числе: широкое признание того, что в современную эпоху национальная безопасность и экономическое благополучие стран в значительной степени зависят от способности обеспечивать безопасность национальной информационной инфраструктуры и цифровой экономики; необходимость обеспечения кибербезопасности на самых высоких уровнях государственного и корпоративного управления; обязательное обеспечение защиты и безопасности наиболее важных объектов инфраструктуры и основных услуг; обязательность разработки и внедрения надлежащих нормативно-правовых требований в области защиты общества от киберпреступлений, перебоев в функционировании сервисов (оказании услуг) и разрушения собственности; необходимость сотрудничества между государственным и частным секторами, а также между международными и региональными сообществами в целях обеспечения принятия эффективных стратегий управления рисками и обеспечения отказоустойчивости в сфере ИКТ, а также обязательство развивать необходимый национальный потенциал для повышения доверия и безопасности в сфере ИКТ, устранения недостатков и реагирования на значительные риски в области кибербезопасности.

Повышение «киберготовности» для управления рисками

Несмотря на наличие разных моделей и механизмов для диагностики, оценки и снижения киберрисков на национальном уровне, а также несмотря на многочисленные призывы со стороны профессионалов отрасли и экспертов кибербезопасности к решительным действиям в этом направлении, повышение уровня кибербезопасности на уровне государств по-прежнему остается нерешенной проблемой. Голландия, например, признав, что ее будущее экономическое здоровье зависит от хорошо налаженной, пользующейся доверием цифровой экономики, стала выделять на это соответствующие средства и создала центр для обеспечения достижения этих целей в условиях безопасности. В июле 2015 года национальный координатор по вопросам безопасности и борьбы с терроризмом провел «Обзор нормативной политики в отношении критически важной инфраструктуры». В этом обзоре дано определение критической инфраструктуры «как комплекса продуктов, услуг и лежащих в их основе процессов, которые необходимы для функционирования страны», и обоснована необходимость «обеспечения ее безопасности и способности выдерживать любые опасности и быстро ликвидировать из последствия».[21] Однако, когда порт Роттердам – крупнейший в Европе – значительно пострадал от атаки с применением вредоносной программы NotPetya в 2017 году, официальные лица Нидерландов, изучив

состояние зависимости порта от ИКТ, обнаружили, что его инфраструктура фактически не была отнесена к категории «критически важной» в национальной стратегии кибербезопасности и не учитывалась в нормативных установках по защите важнейших инфраструктурных систем.

В то же время даже такие страны, как Великобритания, которые определили конкретные критические отрасли – например, здравоохранение, – не ожидали, что поставщики медицинских услуг не будут вкладывать средства в актуализацию своего программного обеспечения и защищу пациентов от киберрисков. Поэтому, когда 81 из 236 национальных учреждений здравоохранения стало жертвой простейшего вируса с требованием выкупа – WannaCry, чего можно было бы легко избежать, произошел инцидент, который в конечном итоге поставил под угрозу много жизней. В результате Великобритании пришлось разбираться с состоянием кибербезопасности и решать, необходимы ли дальнейшие регулирующие меры для повышения эффективности управления рисками в интересах страны и ее граждан.

Как уже говорилось ранее, Германия и США установили небольшое число хозяйствующих субъектов, создающих не менее 2 процентов ВВП страны и заслуживающих дальнейшей защиты со стороны государства и расширения обмена информацией и других форм сотрудничества с ним. Однако взаимодействие с государством не уберегло эти компании от разрушительного воздействия вредоносной программы NotPetya. При том что в этих двух странах работают процессы обмена информацией и данными разведки об угрозах и уязвимостях с крупными частными компаниями, в этом конкретном случае, однако, компании не были оповещены о неминуемой угрозе. В результате серьезно пострадали американские и германские компании, которые оказались не «боеготовыми» перед лицом киберугроз в условиях дефицита адекватной поддержки со стороны соответствующих государства, что привело к длительным срывам в электронной торговле в мировом масштабе. Наконец, ключевые компании ТЭК Саудовской Аравии, которые поставляют почти 25 процентов мирового сжиженного природного газа и других видов топлива для транспортных систем, из-за вредоносной деятельности в сфере ИКТ были отключены от информационно-коммуникационных сетей и оказались в автономном режиме, что в конечном итоге вызвало срывы в функционировании мировых хозяйственных и транспортных систем.

Как показывают рассмотренные примеры, ни одна страна не является «боеготовой» в смысле информационной безопасности, и готовность эта должна начинаться с утверждения дисциплинированного подхода к управлению рисками. Эффективное управление рисками требует от каждого государства, в первую очередь, четкого понимания своих основных ценностей, определения приоритетов защитных мер и демонстрации своей готовности выделять на это в необходимых объемах политический капитал, усилия руководства, финансовые и другие ресурсы.

Например, Колумбия стала применять основанный на управлении рисками подход для оценки своей киберготовности и повышения доверия общества к использованию цифровой среды. Предпринятые меры были нацелены на выполнение задач, поставленных в рамках Национальной политики цифровой безопасности Колумбии (Национальной стратегии кибербезопасности), которая была утверждена Национальным советом цифровой безопасности в апреле 2016 года и оформлена документом «CONPES 3854» от 2016 года. За основу колумбийской политики в сфере кибербезопасности было принято Руководство по управлению рисками ОЭСР наряду с рекомендациями ОАГ, МСЭ и НАТО по оценке угроз в сфере ИКТ и выявлению критически важных объектов, находящихся под угрозой.[22]Исследование послужило стимулом для выявления наиболее актуальных киберрисков, оценки влияния инцидентов в сфере ИКТ на колумбийские организации как в частном, так и в государственном секторах, а также для включения проблематики кибербезопасности в категорию приоритетов как важного фактора социально-экономического развития страны. Проделанная работа также помогла повысить осведомленность различных заинтересованных сторон в стране о распространенных и уникальных видах киберинцидентов, угроз и атак, затрагивающих государственные организации и [частные] предприятия, и позволила приступить к их экономической оценке. Колумбия признала, что управление киберрисками на национальном уровне является важнейшим условием цифровизации всех сторон жизни страны.

Как показывает опыт Колумбии, управление рисками начинается с лидерства и управления. Бóльшая часть разработанных механизмов, индексов и методических руководств, опубликованных в последние годы различными межправительственными организациями, научно-исследовательскими учреждениями, экспертными сообществами, придают фундаментальное значение оценке того, что действительно подвержено риску, и возведению задач кибербезопасности в разряд приоритетных направлений стратегии государственной безопасности. Однако недостаточно включить кибербезопасность в категорию приоритетов в качестве отдельного направления и рассматривать ее в качестве проблемы преимущественно национальной безопасности. Ведь обеспечение кибербезопасности также тесно связано с интегрированностью в сети «Интернет» и быстрым внедрением ИКТ, что может привести – в условиях надежности и отказоустойчивости – к экономическому росту и процветанию. Следовательно, не менее важным является согласование экономических инициатив с актуальными проблемами безопасности, развития и выживаемости при проведении стоимостной оценки рисков и формировании национальной стратегии, предусматривающей меры по снижению рисков.

Оценка рисков

Национальные лидеры должны четко заявить о своем намерении использовать открытую цифровую среду в интересах экономического и социального процветания путем снижения общего уровня рисков цифровой безопасности как внутри своих стран, так и за их

пределами. При этом следует помнить о том, что риски с течением времени изменяются вследствие действий, предпринимаемых, по меньшей мере, двумя участниками – злоумышленником, применяющим инструменты ИКТ для проведения своих атак, и его объектом, который может принять меры предосторожности в целях предупреждения опасности или выхода их нее. Национальным лидерам необходимо продемонстрировать свою приверженность снижению риска и повышению устойчивости путем проведения постоянных оценок рисков как на общенациональном, так и на отраслевом уровне и принятия соответствующих мер политики и процессов для управления выявленными рисками.

Для достижения этих комплексных целей национальные лидеры, ответственные руководители и другие соответствующие заинтересованные стороны каждой страны должны тесно сотрудничать между собой в деле оценки рисков. Определению состояния готовности страны к киберрискам будет способствовать стратегическое планирование и поиск ответов на следующие вопросы:

- Какова краткосрочная и долгосрочная стратегия для страны, включая промышленную политику, экономические цели и приоритеты национальной безопасности?
- Что может угрожать достижению этих целей? Другими словами, какими слабыми местами (например, неучтенными активами с высокой стоимостью) могут воспользоваться недоброжелатели, чтобы сорвать достижение поставленных целей?
- Существуют ли четкие каналы подотчетности и ответственности для обеспечения достижения целей страны и выполнения мер по снижению рисков?
- Находятся ли вопросы кибербезопасности и живучести в центре процесса планирования?

Проведение такой всеобъемлющей оценки позволит выявить наиболее важные направления цифровой зависимости страны (предприятий, служб, инфраструктур, активов) для заблаговременного принятия мер защиты от ущерба, который может иметь серьезные последствия для экономики и безопасности страны.

Снижение риска путем тщательного планирования

Проведя оценку рисков, страна может разработать план снижения рисков в целях приведения текущего состояния кибербезопасности в соответствие с национальными задачами в сфере ИКТ в интересах устранения недостатков и обеспечения будущих приоритетов страны в области экономики и безопасности. При этом такая работа риска должна проводиться силами отдельного компетентного органа страны, специализирующегося на вопросах кибербезопасности. При этом такой орган должен быть сформирован на достаточно высоком уровне системы государственного управления и наделен соответствующими руководящими полномочиями для согласования всех действий

в сфере информационной безопасности, ведения контроля за их реализацией и несение ответственности за допущенные недостатки и достигнутые результаты. Учитывая тот факт, что кибербезопасность охватывает множество различных областей (например, права человека, экономическое развитие, торговлю, контроль над вооружениями, технологии двойного назначения, безопасность, стабильность, мир и разрешение конфликтов), важно обеспечить, чтобы такой национальный компетентный орган обладал необходимой полнотой власти для привлечения как можно более широкого круга заинтересованных сторон и руководства ими, а также был должным образом подотчетен за свои действия.

Даже при наличии множества методик сокращения рисков, о чем свидетельствуют изложенные в предыдущих разделах механизмы, национальным правительствам следует приложить еще более активные усилия для понимания особенностей киберрисков и конкретных угроз, стоящих перед их сетевыми инфраструктурами. Все это должно быть четко описано в национальных концепциях (доктринах, стратегиях) информационной безопасности и в национальных оценках киберрисков. На этой основе предстоит работать со всеми соответствующими заинтересованными сторонами в интересах улучшения планов защиты и оптимизации выделения людских и финансовых ресурсы в целях минимизации этих рисков. Общие стратегии эффективного смягчения киберрисков включают:

- Доведение до всех – от руководителей государства до простых граждан – информации о масштабах киберугроз и повышение общей осведомленности о рисках на всех уровнях. Ценить безопасность помогает понимание степени подверженности рискам нашей повседневной деятельности (а не только личной информации). Поэтому государство должно инициировать общенациональную кампанию по повышению уровня осведомленности общественности, просвещению населения о рисках, связанных с ИКТ, развитию навыков «кибергигиены» и усилению чувства ответственности граждан за формирование сильной культуры кибербезопасности.
- Выявление и ранжирование по приоритетности высокоценных систем (предприятий, служб, инфраструктур, активов), требующих повышенного уровня защиты, и выделение необходимых ресурсов на это; понимание их уязвимости и принятие первоочередных мер безопасности, соизмеримых с экономическими и социальными рисками.
- Разработку соответствующих нормативно-правовых основ защиты общества от киберпреступлений, перебоев с функционированием сервисов и оказанием услуг, а также разрушения собственности.
- Применение широкого диапазона инструментов, включая нормативные требования, законодательство, нормы, стандарты, рыночные стимулы, схемы добровольного соблюдения и другие инициативы, в целях повышения доверия и безопасности в сфере ИКТ, а также устранение недостатков, выявляемых в процессах и продуктах (например, Директива ЕС, Закон Китая «О кибербезопасности», механизмы NIST).

- Повышение осведомленности об обстановке, постоянное отслеживание угроз в сетевому обществу, оповещение о них и применение новейших технологий для обнаружения, отражения и сдерживания таких угроз.
- Развитие необходимых национальных сил и средств для повышения готовности, обеспечения непрерывности планирования, адекватного реагирования на существенные риски в области кибербезопасности и ликвидации последствий крупномасштабных кризисов в сфере ИКТ.
- Привлечение международного сообщества к повышению общей безопасности, надежности и отказоустойчивости совместимых сетей (например, финансовых, телекоммуникационных, энергетических и т.д.) путем разработки глобальных стандартов безопасности и продвижения многосторонних соглашений.
- Оценка образования новых уязвимостей в связи с появлением новых технологий и, с другой стороны, изыскание путей превращения их в возможности повышения безопасности, надежности и отказоустойчивости инфраструктур и активов следующего поколения.

Для эффективного выполнения этих задач и выполнения других мероприятий потребуется четкое определение и разъяснение ролей, обязанностей, процессов, прав на принятие решений и механизмов подотчетности. Для достижения успешных результатов необходимо установить целевые показатели эффективности для различных министерств и ведомств, учреждений или отдельных исполнителей, ответственных за конкретные задачи в принятом плане действий.

Конечно, мероприятия по снижению риска требуют также особого выделения соответствующих ресурсов на их реализацию. Дефицит источников финансирования может подорвать намеченную работу и снизить уровень подотчетности организаций, которым поручено обеспечивать кибербезопасность страны в условиях недостаточного обеспечения необходимыми ресурсами. Под ресурсами подразумеваются финансовые средства, люди, техника и оборудование, а также взаимодействие между всеми исполнителями мероприятий по снижению рисков. Выделение ресурсов на достижение целей и выполнение задач в рамках национальных стратегий кибербезопасности не следует рассматривать как одноразовое действие. Эффективное обеспечение кибербезопасности государства предполагает достаточное, последовательное и постоянное финансирование. При этом ресурсы могут выделяться по функциональному (по выполняемым задачам (целям)) или организационному (по государственным структурам, отвечающим за те или иные аспекты кибербезопасности) принципам. Возможно также формирование на центральном уровне отдельного целевого бюджета под задачи кибербезопасности. Как бы ни было организовано финансирование – либо путем объединения средств из разных источников, либо посредством формирования единого межведомственного бюджета, – общая программа должна контролироваться согласно

установленным вехам и четко определенным временным рамкам для обеспечения успешной реализации принятой стратегии.

Постоянная оценка риска

Когда усилия в области кибербезопасности сводятся к единовременной проверке соответствия установленным требованиям вместо того, чтобы обеспечивать оценку рисков на постоянной основе, они обречены на провал. Эффективное управление рисками требует инициативности и упреждения в отслеживании и прогнозировании угроз в отношении уязвимых мест в действующих в цифровой среде стратегически важных компаний, инфраструктурных систем, услуг, активов и их непрерывной оценки. Как указано выше, уже разработан ряд механизмов, позволяющих обеспечивать устранение сбоев в управлении на основе постоянной оценки рисков. Мониторинг и оценка эффективности и успешности снижения рисков и выполнения других мероприятий в области кибербезопасности должны стать частью механизмов управления, реализуемых государством в своей национальной архитектуре кибербезопасности. Непрерывный контроль за ходом выполнения намеченного плана действий способствует внесению необходимых корректировок в него и дальнейшей реализации комплексной стратегии. Механизмы эффективного управления определяют подотчетность и ответственность за успешного исполнение, а для оценки выполнения реалистичных целей в установленные сроки следует использовать реализуемые, повторяемые, значимые и меняющиеся во времени ключевые показатели эффективности. При этом такие ключевые показатели эффективности должны соответствовать следующим критериям:

- *Конкретность* – нацеленность на улучшение конкретного направления (области);
- *Измеряемость* – возможность количественно оценить успешность той или иной меры;
- *Достижимость* – определение реалистичных результатов, которые могут быть достигнуты с учетом имеющихся ресурсов;
- *Выполнимость* – четкое представление о подлежащих выполнению действий;
- *Ответственность* – четкое назначение ответственного исполнителя;
- *Привязка ко времени* – четкое установление точного срока достижения искомого результата (искомых результатов).

Хотя ни одна страна не может быть полностью готовой к киберугрозам, и киберриски не могут быть полностью устранены, ими можно и нужно управлять. Киберготовность начинается с эффективного подхода к управлению рисками, который включает в себя четкое понимание функционирующих в цифровой среде высокоценных объектов и стратегически важных систем страны (компаний, инфраструктур, услуг, активов), требующих повышенного уровня защиты. Достижение такого понимания позволит

адекватно оценить имеющиеся уязвимости и принять первоочередные меры безопасности, соизмеримые с экономическими и социальными рисками.

Только при четком согласовании и координации действий со стороны всех заинтересованных субъектов будет возможно значительно снизить киберриски и продвинуться вперед в направлении обеспечения безопасности страны.

Выводы

Сегодня в мире отмечается рост *дефицита* кибербезопасности. Объемы, масштабы и изощренность киберугроз в отношении важнейших функций и инфраструктур опережают темпы принятия мер их защиты. Перед лицом растущих угроз в сфере ИКТ государства обязаны незамедлительно сосредоточить усилия на деле повышения своей киберготовности. Потери неумолимо накапливаются; ущерб растет; опасность – неминуема.

Государства должны разработать всеобъемлющие национальные стратегии кибербезопасности, которые включали бы создание специального компетентного органа, отвечающего за общую национальную политику в области информационной безопасности страны. Необходимо на всех уровнях – от руководства до простых граждан – формировать общегосударственное понимание стоящих перед страной рисков. Каждый должен понимать уязвимость цифровой среды своей страны и знать свою роль в смягчении рисков. Эта стратегическая «дорожная карта» позволяет принять соответствующие меры, политику и процессы для устранения недостатков и снижения рисков для общества, экономики и страны в целом. Этого нельзя добиться без специального выделения соответствующих ресурсов в поддержку инициатив по снижению рисков и повышению устойчивости. При этом одним из наиболее важных шагов в обеспечении безопасности национальной инфраструктуры и услуг в сфере ИКТ, от которых зависит цифровое будущее и экономическое благосостояние современного общества, является принятие национальной стратегии информационной безопасности.

Справка об авторе

Мелисса Хэтэуэй – ведущий эксперт в области регулирования киберпространства и информационной безопасности. В составе администрации президента Дж. Буша-младшего возглавляла работу в рамках Комплексной национальной инициативы по кибербезопасности, а в администрации президента Барака Обамы руководила работой группы по разработке Обзора политики в отношении киберпространства. Основанная Мелиссой Хэтэуэй компания Hathaway Global Strategies LLC консультирует клиентов из государственного и частного секторов, предлагая уникальное сочетание специальных нормативно-технических экспертных знаний в интересах формирования глубокого

понимания всех аспектов информационной безопасности на уровнях государственной политики и социально-экономического развития. Она разработала уникальную методологию оценки и измерения уровня готовности к определенным рискам в области кибербезопасности, известную как «Индекс киберготовности». Вторая версия Индекса (Cyber Readiness Index 2.0) размещена здесь: http://www.potomacinstitute.org/academic-centers/cyber-readiness-index. Из-под пера М. Хэтэуэй регулярно выходят материалы о разных аспектах кибербезопасности, затрагивающих организации и страны. На этих сайтах размещена бóльшая часть ее статей:

http://belfercenter.ksg.harvard.edu/experts/2132/melissa_hathaway.html и https://ctm.columbia.edu/people/melissa-hathaway.

[1] Оксфордский словарь так определяет понятие «риск»: «Риск = Угроза х Уязвимость». CRM: «Риск = Условие (Вероятность) + Последствие (Воздействие)».

[2] Nicolas Rapp and Robert Hackett, "A Hackers Toolkit." *Fortune Magazine* 25 October 2017, http://fortune.com/2017/10/25/cybercrime-spyware-marketplace/

[3] Eduard Kovaks, "Shadow Brokers Want $20,000 for Weekly Leaks," *Security Magazine,* 30 May 2017, https://www.securityweek.com/shadow-brokers-want-20000-monthly-leaks; and
Eduard Kovaks, "Shadow Brokers Promise More Exploits for Monthly Fee," *Security Magazine,* 16 May 2017, https://www.securityweek.com/shadow-brokers-promise-more-exploits-monthly-fee; and
Nicole Perloth, "A Cyberattack the 'World Isn't Ready For,'" The New York Times, 22 June 2017, https://www.nytimes.com/2017/06/22/technology/ransomware-attack-nsa-cyberweapons.html?_r=0

[4] National Audit Office, "Investigation: WannaCry cyber-attack and the NHS," 27 October 2017, https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/.

[5] Richard Chirgwin, "IT 'heroes' saved Maersk from NotPetya with ten-day reinstallation bliz," *The Register,* 25 January 2018, https://www.theregister.co.uk/2018/01/25/after_notpetya_maersk_replaced_everything/.

[6] A.P. Moller-Maersk, Balersdorf, DHL, DLA Piper, Federal Express, Merck, Mondolez, Nuance, Reckitt Benckiser Group, Rosneft, Saint Gobain, and WPP. Lloyds of London, "Extreme Cyber-Attack Could Cost as Much as Superstorm Sandy," 17 July 2017, https://www.lloyds.com/news-and-risk-insight/press-releases/2017/07/cyber-attack-report.

[7] Kelly Jackson Higgins, "Schneider Electric: TRITON/TRISIS Attack Used 0-Day Flaw in its Safety Controller System, and a RAT," *Dark Reading,* 18 January 2018, https://www.darkreading.com/vulnerabilities---threats/schneider-electric-triton-trisis-attack-used-0-day-flaw-in-its-safety-controller-system-and-a-rat/d/d-id/1330845.

[8] Melissa Hathaway, "Falling Prey to Cybercrime: Implications for Business and the Economy," in *Securing Cyberspace: A New Domain for National Security,* February 2012, Aspen Institute Press.

[9] Many countries have different definitions of critical infrastructures. For the purposes of this paper, a broad definition was used. See: Homeland Security Digital Library, "Presidential Decision Directive 63, PDD/NSC-63," 22 May 1998, https://fas.org/irp/offdocs/pdd/pdd-63.htm.

[10] Yanqing Hong, "The Cross-border Data Flows Security Assessment: An Important Part of Protecting China's Basic Strategic Resources," 20 June 2017, Yale Law School, Paul Tsai China Center Working Paper, https://law.yale.edu/system/files/area/center/china/document/dataflowssecurity_final.pdf.

[11] NIST, "Cybersecurity 'Rosetta Stone' Celebrates Two Years of Success," 18 February 2016, https://www.nist.gov/news-events/news/2016/02/cybersecurity-rosetta-stone-celebrates-two-years-success.

[12] Hathaway Global Strategies LLC. Insights from engagement with Board of Directors and Management of affected companies.

[13] NIST, "NIST Special Publication 800-37 (Rev. 2) DRAFT — Risk Management Framework for Information Systems and Organizations: A System Lifecycle Approach for Security and Privacy (Discussion Draft)," September 2017, https://csrc.nist.gov/CSRC/media/Publications/sp/800-37/rev-2/draft/documents/sp800-37r2-discussion-draft.pdf.

[14] WSIS, Geneva 2003 - Tunis 2005, "Tunis Commitment," 18 November 2005, http://www.itu.int/net/wsis/docs2/tunis/off/7.html.

[15] ITU (2014), Global Cybersecurity Index, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx.

[16] OECD (2015), Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris, https://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf.

[17] WEF (2018), Cyber Resilience Playbook for Public-Private Collaboration, pp. 33-36, https://www.weforum.org/reports/cyber-resilience-playbook-for-public-private-collaboration.

[18] Ibid.

[19] Melissa Hathaway, "Cyber Readiness Index 1.0," *Hathaway Global Strategies LLC* (2013), *http://belfercenter.ksg.harvard.edu/ les/ cyber-readiness-index-1point0.pdf*.

[20] NCSI, "NCSI Methodology," http://ncsi.ega.ee/methodology (1.0) and http://ncsi.ega.ee/ncsi-methodology-2-0-launched/ (2.0).

[21] National Coordinator for Security and Counterterrorism, "Review of Policy on Critical Infrastructure," July 2015; and Melissa Hathaway and Francesca Spidalieri, "The Netherlands Cyber Readiness at a Glance," May 2017, Potomac Institute for Policy Studies, http://www.potomacinstitute.org/images/CRI/FinalCRI20NetherlandsWeb.pdf.

[22] OAS, MINTIC, IDB (2017), Impact of Digital Security incidents in Colombia 2017, https://publications.iadb.org/handle/11319/8552.