КИБЕРГОТОВНОСТЬ ГЕРМАНИИ: КРАТКИЙ ОБЗОР

Ведущий исследователь: Мелисса Хатауэй

Крис Демчак, Джейсон Кербен, Дженнифер МакАрдл, Франческа Спидальери

Октябрь 2016

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
Е-почта: CyberReadinessIndex2.0@potomacinstitute.org

Follow us on Twitter: @CyberReadyIndex

Графическое оформление обложки: Алекс Талиесен

Благодарность:

Потомакский институт политических исследований и авторы выражают благодарность следующим лицам: г-ну Арн Шенбому, президенту Германского федерального офиса по информационной безопасности ((Bundesamt für Sicherheit in der Informationstechnik, BSI), исполнительному руководству BSI, а также д-ру Сандро Гайкену, директору Института цифрового общества при Европейской школе управления и технологии (ESMT), г. Берлин. Авторы также благодарны Алексу Талиесену за оформление обложки и Шерри Лавлес за редакторскую и оформительскую работу.

Публикация русскоязычной версии доклада осуществлена DR Analytica (analytica.digital.report) в партнерстве с Фондом SecDev (Оттава, Канада). DR Analytica – экспертная, информационно-аналитическая группа, специализирующаяся в области безопасности, регулирования и управления киберпространства. Фонд SecDev – один из признанных мировых лидеров в изучении кибербезопасности, почти двадцать лет тесно сотрудничающий с государственными, частными и общественными организациями постсоветского пространства в деле продвижения безопасного использования информационно-телекоммуникационных технологий во всех сферах жизни.

КИБЕРГОТОВНОСТЬ ГЕРМАНИИ: КРАТКИЙ ОБЗОР

СОДЕРЖАНИЕ

КИБЕРГОТОВНОСТЬ ГЕРМАНИИ

КРАТКИЙ ОБЗОР

Население	81,4 млн
Прирост населения	0,5%
ВВП в рыночных ценах (по текущему курсу доллара США)	$ 3,356 трлн
Рост ВВП	1,7%
Год появления Интернета	1983
Год принятия Национальной стратегии кибер-безопасности	2011
Национальные доменные зоны	.de
Количество пользователей фиксированного широкополосного доступа на 100 пользователей интернета	35,8
Количество контрактов на мобильный широкополосный доступ на 100 пользователей интернета	63,6
Количество мобильных номеров на 100 пользователей	120,4

Развитие Информационно-коммуникационных технологий (ИКТ) и степень развития коммуникаций в стране

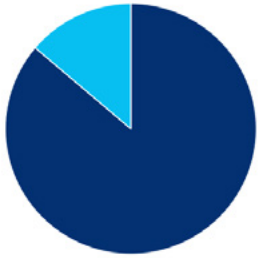
Позиция в Индексе развития ИКТ (IDI) Международного союза электросвязи (МСЭ)	15	Индекс сетевой готовности (NRI) Всемирного экономического форума	13

Источники: World Bank (2015), International Telecommunications Union (2015), WEF Network Readiness Index (2015), and Internet Society.

ВВЕДЕНИЕ

Интернет стал впервые доступен в Германии в 1983 году, когда появилась Bildshirmtext (BXT) – одна из первых услуг по передаче данных от государственной корпорации Deutsche Telekom. Спустя год в Германию прибыло первое электронное сообщение из США, содержавшее текст «Willkommen CSNET». Это послужило моментом официального открытия интернета в Германии.[1] Deutsche Telekom являлся единственным интернет-провайдером в Германии вплоть до 1995 года, когда доступ к возможности оказания таких услуг был открыт для всех компаний на рынке. После приватизации Deutsche Telekom, государство и сменяющие друг друга правительства продолжали контролировать примерно треть его акций,[2] а компания до сего момента остается ведущим интернет-провайдером в стране.

Сегодня Германия – один из мировых лидеров в области создания технологически современных телекоммуникационных систем, что стало результатом значительного объема инвестиций с момента объединения страны в 1990 г, а уровень использования интернета в стране достигает 86%. Правительство ФРГ активно способствовало развитию ИКТ и росту абонентской базы интернета с самого момента его появления и стало первопроходцем в рамках многих проектов в области телекоммуникаций. Германия стала первой страной в мире, которая оцифровала свои библиотеки после появления глобальной сети. Немецкий проект цифровых библиотек «Global Info» стартовал в 1998 году как часть более масштабной программы «Информация как сырье для инноваций» (Information as Raw Material for Innovation). Целью этого крупного проекта было развитие сотрудничества с университетами, издательствами, книжными торговыми домами, информационными центрами и научными сообществами, а также с академическими и исследовательскими библиотеками и архивами.[3]



Уровень испольования интернета в Германии: 86% населени

Германия также стала первой в Европе страной, выделившей частоту в 700 МГц для широкополосного мобильного доступа в интернет в 2016 году. В настоящее время только 20% сельской местности в ФРГ имеет доступ к широкополосной связи, «Цифровая повестка дня на 2014-2017 гг.» (Digital Agenda 2014-2017) ставит цель решить эту проблему посредством развертывания сети широкополосного мобильного доступа в труднодоступных и удаленных местностях и предоставить возможность для всех домохозяйств получить доступ на скорости как минимум 50 мегабит в секунду к 2018 г.[4] Кроме того, надо

отметить, что в Германии активно развивается использование протокола IPv6, и уровень его использования достиг 10% по сравнению с всего 3,5% в других развитых странах (по состоянию на апрель 2014 г.).

Стратегия ИТ развития Германии очевидно сконцентрирована на развитии конкуренции, экономическом росте и социальном благосостоянии в стране. В ней отмечается, что развитие сетей высокоскоростного доступа и доверия к ИКТ технологиям повысит «инновационный потенциал для достижения дальнейших роста и развития».[5] Эта стратегия предусматривает, что Германия станет лидером Интернет-экономики с использованием ИКТ и автоматизации в промышленности, а также при помощи содействия инвестициям в информационно-коммуникационные технологии, исследования в области кибер-безопасности, микроэлектроники и в других смежных областях. Размер ИКТ рынка Германии – крупнейшего в Европе и четвёртого по объему в мире – облегчит достижение этих амбициозных планов.[6]

Тем не менее, в Белой книге Министерства обороны 2016 г. (German Defense White Paper) указываются все недостатки и угрозы ввиду того, что Германия – страна средних масштабов, как в географическом, так и в демографическом смыслах, и ей приходится существовать в быстро меняющемся мире. Несмотря на то, что экономика Германии – четвертая по величине в мире, правительство осознает, что «вероятность того, что такая ситуация сохранится – невелика».[7] В документе признается, что между национальной безопасностью и экономическим благосостоянием общества знания в XXI веке существует прямая взаимосвязь. В документе также указывается, что «знание является стратегическим ресурсом Германии» ввиду ее зависимости от «безопасных путей поставок, стабильности рынков, а также устойчивого функционирования информационно-коммуникационных систем», а также что «такого рода зависимость будет только нарастать».[8]

Начиная с 2011 года правительсво Германии активно содействовало развитию того, что оно называет «четвертой промышленной революцией» под лозунгом Industrie 4.0. Этот проект являлся частью «Плана действий стратегии высоких технологий – 2020» (High-Tech Strategy 2020 Action Plan).[9] Эта инициатива стимулирует частные компании пользоваться тенологиями интернета вещей, и это в большей мере касается 3,6 милионов малых и средних предприятий, которые создают до 60% рабочих мест в стране и производят до двух третей от ее почти 4-триллонного ВВП.[10] Правительство планирует инвестировать 200 млн евро (примерно 222 млн. долларов США) в развитие программы Industrie 4.0, а также в научные исследования в ее рамках в правительственных, академических и бизнес-организациях для того,

чтобы использовать возможности телекоммуникаций для повышения качества, снижения цен, повышения эффективности и роста экономики. Канцлер Ангела Меркель призвала все остальные страны Европы также присоединиться к этой инициативе. Во время ее речи на Всемирном экономическом форуме в Давосе в 2015 г., она заявила, в частности: «Те, кто будут лидерами в ИКТ, займут лидерские позиции и в промышленном производстве... и эту гонку мы пока еще не выиграли».[11]

Являясь лидером в развитии и внедрении ИКТ технологий, Германия также сталкивается с высоким уровнем кибер-преступности, промышленного шпионажа, умышленного нарушения критически важных сервисов, а также других вредоносных действий в киберпространстве. В 2012 г. ассоциация промышленников оценивала ущерб экономике Германии от кражи интеллектуальной собственности в размере 1,5% от ВВП страны. В 2013 году, по экспертным оценкам, двое из пяти интернет-пользователей в Германии стали жертвами кибер-преступлений, и большое количество компаний и правительственных органов стали жертвами кибер-атак.[12] Реагируя на рост объема, масштабов и серьезности кибер-преступности, правительство Германии заявило о намерении защитить национальные инвестиции и экономическую безопасность страны, особенно в отношении персональной информации граждан и защиты других данных.[13] Тем не менее, инвестиции в программу Industrie 4.0 в области обеспечения кибер-безопасности и создания инновационных технологий, направленных на преодоление потенциальных ИТ-угроз, в настоящее время, все еще ограничены.[14]

Германия является лидером в европейском диалоге по вопросам защиты информации и одновременном свободном международном перемещении товаров, услуг, рабочей силы, капитала и данных. Эти цели являются основополагающими в рамках инициативы Единого европейского цифрового рынка (European Digital Single Market), а также чрезвычайно важны для экономического здоровья и благосостояния Германии и всей Европы. Германия будет принимать саммит Большой двадцатки в Гамбурге в 2017 году, и с большой вероятностью, использует это событие для того, чтобы подчеркнуть необходимость того, чтобы каждая страна развивала свои способности в деле противостояния кибер-угрозам.

Для оценки готовности Германии к преодолению кибер-рисков использовался Индекс кибер-готовности (CRI) 2.0. Приведенный ниже анализ содержит базовые исходные данные, которые позволят Германии лучше понять степень уязвимости и зависимости от интернет-инфраструктур, а также оценить

свою готовность и приверженность развитию в направлении от нынешнего состояния дел к полной реализации национальных кибер-возможностей для поддержания и развития своего будущего в киберпространстве. Ниже приводится полная оценка деятельности и возможностей страны на основе семи основных элементов CRI 2.0 (Национальная стратегия, реагирование на инциденты, кибер-преступность и охрана правопорядка, обмен информацией, инвестиции в исследования и разработки, дипломатия и торговля, а также оборона и кризисное реагирование):

Оценка киберготовности Германии (2016)

1. НАЦИОНАЛЬНАЯ СТРАТЕГИЯ

В 2008 году правительство Германии отреагировало на рост количества зараженных вирусами устройств и количества кибер-преступлений в стране, предоставив гражданам CD диски, с помощью которых они могли провести чистку от вредоносных вирусов своих компьютеров и других устройств. В этой связи было отмечено, что защита страны является обязанностью граждан. К 2011 году правительство приняло более систематичный и централизованный подход, опубликовав первую версию документа «Кибер-безопасность для Германии» (Cyber Security Strategy for Germany).[15] Этот документ признает зависимость между ИКТ и экономическим и социальным ростом в стране и указывает, что интернет, а также ИКТ технологии являются критической инфраструктурой для Германского общества.[16]

К 2011 году правительство приняло более систематичный и централизованный подход, опубликовав первую версию документа «Кибер-безопасность для Германии», в котором признает зависимость между ИКТ и экономическим и социальным ростом в стране.

Национальная стратегия кибер-безопасности выделяет несколько стратегических областей и целей для более успешной борьбы с кибер-угрозами, в т.ч.: защита критических элементов инфраструктуры и ИТ систем; защита ИТ-систем общественного управления посредством создания единой «федеральной сети»; создания Национального центра кибер-реагирования (National Cyber Response Center) для реагирования на инциденты и защиты данных и систем; создание Совета национальной кибер-безопасности (National Cyber Security Council) для активизации сотрудничества между организациями государственного и частного сектора; развитие активного международного сотрудничества для координации деятельности по обеспечению кибер-безопасности; разработка и создание надежных ИТ-продуктов с использованием инноваций; подготовка и тренинг персонала федеральных органов власти; а также эффективное использование инструментария государственных органов – таких как законодательство – для борьбы с кибер-преступностью.

Кроме того, указанный документ определил Федеральный офис информационной безопасности Министерства внутренних дел

(Bundesamt für Sicherheit in der Informationstechnik, BSI) органом, ответственным за кибер-безопасность страны, а также ответственным за реализацию указанной стратегии.[17] BSI был создан в 1991 году для предоставления услуг в области ИТ-безопасности федеральному правительству, ИКТ-компаниям, частным и коммерческим пользователям, а также интернет-провайдерам Германии. Как требовала Национальная стратегия, BSI создал Национальный центр кибер-реагирования (Nationales Cyber-Abwehrzentrum, NCAZ), ответственный за определение, анализ и разработку мер, необходимых для нивелирования и устранения потенциальных угроз.[18]

В соответствии с Национальной стратегией кибер-безопасности от 2011 года, был также создан Национальный совет кибер-безопасности, целью которого было позволить секретариатам всех министерств внести вопросы кибер-безопасности в стратегии реализации всех политических направлений деятельности в стране. Совет также координирует применение единых для государственного и частного секторов превентивных мер и междисциплинарных подходов в области кибер-безопасности. Помимо представителей центрального правительства и земель Германии в Совет входят также представители каждого министерства (в т.ч. обороны, внутренних дел, экономики и технологий и других). На заседания в качестве ассоциированных членов часто приглашаются представители частного бизнеса. В 2012 году BSI, для содействия реализации широких политических задач, совместно с Федеральной ассоциацией информационных технологий и новых средств коммуникации (BITKOM) создали некоммерческую организацию – Альянс за кибер-безопасность (Alliance for Cyber Security). Основной его миссией является упрочение кибер-безопасности в Германии и повышение устойчивости страны против кибер-атак. В настоящее время Альянс занимается сбором всесторонней базы данных, а также поддержкой обмена знаниями и опытом.[19] С момента своего создания в 2012 году, Альянс значительно увеличился, как в плане количества объединенных им организаций, так и в плане количества партнеров, с которыми он сотрудничает.

Цифровая повестка Германии от 2014 года (Digital Agenda 2014-2017) повторяет основные элементы Национальной стратегии кибер-безопасности, также признавая важность ИКТ для экономического роста, одновременно подчеркивая необходимость роста уровня безопасности в киберпространстве. «Цифровая повестка» также отмечает, что половина германских интернет-пользователей не уверены в безопасности своих данных в интернете, т.к. доверие к ИКТ-технологиям жизненно важно для развития цифровых коммуникаций,

электронной коммерции и создания Единого европейского цифрового рынка, правительство крайне озабочено такими статистическими данными и предприняло серьезные шаги для повышения интернет-безопасности граждан.[20] Так, BSI в настоящее время работает над реализацией Акта об ИТ безопасности от 2015 года (IT Security Act) – ключевым элементом национальной стратегии ИТ-развития, и ее положениям по защите критической инфраструктуры национального значения.[21] Эта деятельность включает в себя постоянное сотрудничество с операторами этих критически важных элементов инфраструктуры с целью определения минимальных стандартов уровня безопасности для таких компаний и в целом секторов экономики, а также с целью повышения доступности, адекватности, конфиденциальности и целостности системы ИТ-безопасности по всей стране.

Для того, чтобы повысить уровень ИКТ-безопасности и устойчивости, как стратегия кибер-безопасности, так и «цифровая повестка» пытаются создать всеобъемлющий и многосторонний подход в деле повышения безопасности онлайн-услуг и критически важных элементов инфраструктуры. Тем не менее, правительству Германии многое еще предстоит сделать для повышения уровня координации и взаимодействия между ведущими государственными и частными организациями, а также национальными ИТ-системами для того, чтобы быть более подготовленными к новым рискам, связанным со все растущей компьютеризацией критически важных услуг в национальной экономике.

2. РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ

Являясь органом, ответственным за национальную кибер-безопасность Германии, BSI формирует политику и план действий в области информационной безопасности в рамках всего правительства и всей страны для предотвращения, определения и реагирования на инциенты, а также является ведущим подотчетным органом в правительстве по вопросу кибер-инцидентов. BSI выпускает предупреждения и оповещения о вирусах и вредоносных программах в ИТ-продуктах и услугах, распространяет информацию как для заинтересованных организаций, так и для общественности, а также дает рекомендации по противодействию вредоносным программам и действиям.[22] BSI также несет ответственность за организацию информационного обмена с более чем 50 000 негосударственных и частных организаций. Несмотря на то, что система раннего оповещения BSI еще не полностью завершена, она повторяет структуру и основные элементы системы оповещения, которую использует Центр информационного обмена и анализа финансовых органов США (FS-ISAC).[23]

Многочисленные команды экстренного реагирования (CERTs) и подобные им организации создавались в Германии с 1991 года. В 1994 году BSI создает свою собственную команду экстренного реагирования (BSI-CERT) для обслуживания федеральных агентств и ориентированную в основном на сбор информации. В 2001 году BSI-CERT был преобразован в правительственную команду и получил название CERT-Bund. За прошедшее время CERT-Bund превратился в настоящую национальную структуру, которая служит платформой и центральным контактным узлом для превентивных, проактивных мер, а также действий по реагированию на кибер-инциденты. Сегодня CERT-Bund тесно сотрудничает с государственными и негосударственными командами по широкому кругу вопросов. Он активно занимается мониторингом с целью предупреждения инцидентов, по желанию партнеров, их сфер ответственностей, в том числе это касается и поставщиков, и производителей ИТ-решений, а также частных и коммерческих пользователей. Он также готовит и рассылает предупреждения, предоставляет информационные услуги, а также ведет базу данных и лог инцидентов в области кибер-безопасности.[24] В 2006 году BSI также создало «Гражданский» CERT (Bürger-CERT) специально для повышения осведомленности общественности и малого бизнеса в вопросах кибер-безопасности.[25]

Федеральный офис информационной безопасности Германии (BSI) – национальный орган кибер-безопасности и центр реагирования на инциенты.

Несмотря на то, что в Германии нет единого сводного национального плана реагирования на инциденты, существует два документа: «Национальный план защиты информационной инфраструктуры» (National Plan for Information Infrastructure Protection) от 2005 года, актуальный как для правительства, так и для бизнеса, и «План реализации защиты критических элементов инфраструктуры» (Critical Infrastructure Protection (CIP) Implementation Plan) от 2007 года, определяющий стратегию реагирования на кризисы в сфере ИТ, и содержащий рекомендации бизнес-сообществу в плане реализации определенных процессов в случае крупных кибер-инцидентов.[26] В соответствии с последним планом (от 2007 г.), операторы критических элементов инфраструктуры уже «создали и применяют соответствующие процедуры раннего оповещения, в раках которых четко определяются структуры и лица, информируемые в

первую очередь после определения кризисной ситуации, а также содержатся критерии дифференциации форм и методов оповещения»[27]. Кроме прочего, этот план содержит указания по созданию рабочих групп по различным аспектам кибер-безопасности, таких как кризисное управление, антикризисные учения и постоянная доступность критически важных сервисов. В нем также содержатся указания по структуре соглашений между правительством и частными операторами о создании кризисной информационной структуры и ее функциях по защите критически важных элементов инфраструктуры и реагированию на ИТ-инциденты в области безопасности.

Национальная стратегия кибер-безопасности от 2011 года содержит указания BSI создать Национальный центр кибер-реагирования (Nationales Cyber-Abwehrzentrum, NCAZ), который будет ответственен за координацию деятельности по реагированию на кибер-инциденты между правительством и частным сектором. В роли национального командного, контрольного и аналитического центра NCAZ обеспечит «быстрое реагирование всеми компетентными органами на серьезные инциденты и предоставит анализ таких инцидентов и оценку потенциальных рисков всем соответствующим органам; будет координировать сотрудничество с секторальными и региональными командами по кризисному управлению».[28]

В работе этого контрольного и аналитического центра напрямую и в непосредственном сотрудничестве с компаниями частного сектора принимают участие Федеральная служба защиты Конституции (Bundesamt für Verfassungsschutz, BfV), Федеральная служба гражданской обороны и преодоления последствий катастроф (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, BBK), а также другие государственные органы, ответственные за обеспечение безопасности, в т.ч. Федеральное ведомство уголовной полиции (Bundeskriminalamt, BKA), Федеральная полиция Германии (Bundespolizei, BPOL), Ведомство криминальных расследований таможни (Zollkriminalamt, ZKA), Федеральная разведывательная служба (Bundesnachrichtendienst, BND), Вооруженные силы Германии и др. Повестка развития NCAZ предусматривает дальнейшее расширение возможностей Центра в области экстренного реагирования на угрозы и инциденты.

В Германии были организованы несколько учений национального масштаба в области цифровой безопасности для тренировки реализации планов кризисного реагирования правительственными организациями и операторами критически важных элементов инфраструктуры. Одно из этих учений по реагированию и готовности к кризисным ситуациям в 2011 году, имело своей целью тренировку процедур

реагирования правительственных структур в случае многоуровневой атаки, включая DDoS-атаки в отношении критически важных элементов инфраструктуры, внедрения вирусных программ в банковскую систему, а также имитации несуществующего трафика в рамках системы контроля воздушных передвижений.[29] Германия также принимает участие в международных учениях, организуемых в рамках Европейского Союза и НАТО. Несмотря на количество учений, проведенных в последние годы, план CIP содержит рекомендации «проведения большего количество учений для реализации и совершенствования современных концепций обеспечения безопасности».

Наконец, Федеральная служба защиты Конституции (BfV) – внутреннее разведывательное агентство Германии – публикует ежегодные отчеты о современных угрозах в области информационной безопасности. Отчет 2016 содержит информацию о том, что Россия и Китай являются ведущими источниками кибер-атак в Германии. Также в отчете сообщается, что германские спецслужбы обнаружили возможные кибер-угрозы ряду немецких объектов со стороны Ирана.[30]

3. КИБЕРПРЕСТУПНОСТЬ И ОХРАНА ПРАВОПОРЯДКА

Германия продемонстрировала приверженность делу обеспечения безопасности и борьбы с кибер-преступностью подписав (в 2001 г.) и ратифицировав (в 2009 г.) Международную конвенцию по кибер-преступлениям Совета Европы, также известную, как Будапештская конвенция, а также предприняв ряд шагов для ее реализации в стране. Германия также подписала и ратифицировала Дополнительные протоколы к Конвенции по кибер-преступлениям, которые криминализируют расистскую и ксенофобскую деятельность, осуществленную посредством компьютерных систем. В своей Национальной стратегии кибер-безопасности Германия подтвердила свою приверженность дальнейшим усилиям в области гармонизации международного уголовного права на основе Будапештской конвенции.

В июле 2015 г. в Германии был принят Акт об информационной безопасности (IT Security Act), целью которого является предотвращение ущерба важнейшим ИТ-системам, таким, например, как системы Министерства внутренних дел (BSI), провайдеров телекоммуникационных услуг, операторов критически важных элементов инфраструктуры и др. В настоящее время, BSI занимается реализацией положений этого Акта, который включает в себя минимальные стандарты кибербезопасности для более 2000 критически важных инфраструктурных компаний. В соответствии с законодательством, такие минимальные стандарты безопасности обеспечиваются за счет

развития доступности, аутентичности, конфиденциальности и целостности систем кибер-безопасности во всей стране; повышения уровня интернет-безопасности для граждан; а также повышенного уровня защиты критически важных в национальном масштабе элементов инфраструктуры.[31] Помимо прочего, в Германии действуют и другие законы, запрещающие такие преступные действия, как компьютерное мошенничество, фальсификация данных, компьютерный саботаж, кибер-шпионаж, фишинг, а также другие подобные кибер-преступления, которые, в соответствии с национальным законодательством, преследуются наравне с обычными преступлениями.[32] В течение двух лет после принятия Акта все упомянутые в нем операторы обязаны реализовать необходимые организационные и технические меры безопасности для защиты своих кибер-систем, их компонентов или процессов, имеющих отношение к функционированию таких систем. Среди указанных мер – применение самых современных технологических новинок. Более того, операторы критически важных систем должны проходить процедуру аудита в области кибер-безопасности или процедуру сертификации как минимум каждые два года. Также, они получают возможность самостоятельно предлагать новые стандарты безопасности в своей области деятельности.

Что касается правоохранительной деятельности, в Германии созданы достаточные условия для противодействия различным видам кибер-преступности. NCAZ, BSI и BKA совместно работают в области борьбы с кибер-преступностью в национальном масштабе. В частности, NCAZ объединяет ресурсы различных правительственных агентств, в т.ч. Федеральной полиции и Федеральной разведывательной службы, а также частного сектора.[33]

Национальная стратегия кибер-безопасности 2011 года предусматривает развитие потенциала правоохранительных органов, BSI, а также частного сектора, в области борьбы с кибер-преступностью, а также в области защиты страны от шпионажа и саботажа. В Германии созданы «органы совместного реагирования с участием частного сектора и компетентных правоохранительных органов».[34] Как указывается в Акте об информационной безопасности 2015 года, для успешной реализации указанных задач потребуются дополнительные усилия и дальнейший прогресс. В конце 2017 года станет известно, насколько успешно сотрудничали к этому моменту правительство и частный сектор, чтоб значительно снизить уровень кибер-преступности. Учитывая все сказанное, стоит все же отметить, что остается пока неясным, существуют ли в стране успешные инициативы в области обучения судей, прокуроров, юристов, сотрудников правоохранительных органов, криминалистов, и также других специалистов.

4. ОБМЕН ИНФОРМАЦИЕЙ

Как указывается в Национальной стратегии кибер-безопасности 2011 г., NCAZ несет ответственность как за координацию деятельности по реагированию на инциденты, так и за обмен информацией в этой области. Эта информация включает в себя данные об уязвимостях и слабых местах ИТ-продуктов, виды и формы возможных кибер-атак, данные о потенциальных взломщиках и т.д. Для полноценного выполнения таких обязанностей необходимо создание единого органа, в который бы входили представители бизнеса и других негосударственных организаций, которые могли бы поставлять текущую и актуальную информацию по вопросам кибер-безопасности в национальном масштабе, а также давать рекоме¬¬ндации заинтересованным сторонам по подготовке к реагированию и действиям в случае кибер-инцидентов. Альянс для кибер-безопасности (Alliance for Cyber Security) – платформа для сотрудничества и обмена информацией, созданная в 2012 г. – который сотрудничает с NCAZ, соответствует этим требованиям. Альянс способствует развитию тесного сотрудничества между партнерами, представляющими академические, правительственные и бизнес-круги, а также компании, играющие важную роль в жизни общества.

Содействие информационному обмену оказывает также Национальный оперативный центр информационных технологий (Nationales IT-Lagezentrum), который действует под руководством Министерства внутренних дел, отслеживает вопросы, связанные с кибер-безопасностью в национальном и международном масштабе с тем, чтобы впоследствии оперативно определять и анализировать важнейшие кибер-инциденты и рекомендовать меры по их преодолению. В случае возникновения ИТ-кризиса, возможности и полномочия этого центра могут быть расширены, и он может быть преобразован в Национальный центр реагирования на кризисные ситуации в области информационных технологий (Nationales IT-Krisenreaktionszentrum). Этот центр обладает всеми возможностями для преодоления кибер-кризисов во всех сферах и в национальном масштабе, в том числе он имеет доступ к правительственным сетям и элементам критической инфраструктуры.

NCAZ несет ответственность как за координацию деятельности по реагированию на инциенты, так и за общую безопасность обмена информацией в стране

Помимо прочего, Германия участвует в различных внутрифедеральных и межведомственных объединениях, в целях содействия обмену информацией. Двусторонняя американо-германская группа сотрудничества по вопросам кибер-безопасности (US-Germany Cyber Bilateral Meeting) является признанным органом, который позволяет обмениваться ценными данными между двумя странами.[35] Германия также является членом Национального альянса кибер-криминалистики и киберподготовки (National Cyber Forensics and Training Alliance (NCFTA), некоммерческой корпорации в США, целью которой является развитие сотрудничества между бизнесом, академическими кругами и правоохранительными органами для определения, снижения уровня риска и полной нейтрализации кибер-угроз.[36]

Реализация многих инициатив в области обмена информацией может столкнуться с некоторыми трудностями ввиду того, что в Германии существуют законы и программы федерального и местного уровня. Способности адекватно реагировать на наиболее сложные и серьезные угрозы могут отличаться в различных субъектах федерации ввиду того, что каждая из германских земель обладает различными возможностями в области обеспечения кибер-безопасности и разным уровнем развития соответствующих служб. Обмен информацией критически важен для реализации всех усилий центрального правительства, однако достичь всех поставленных целей в ближайшие сроки будет очень сложно.

5. ИНВЕСТИЦИИ В ИССЛЕДОВАНИЯ И РАЗРАБОТКИ (R&D)

Национальная стратегия кибер-безопасности 2011 г. предусматривает интенсификацию исследований в области кибер-безопасности и защиты критически важных элементов инфраструктуры в качестве одной из стратегических областей развития. Германская «Цифровая повестка» 2014-2017 (Digital Agenda 2014-2017) указывает на необходимость значительных инвестиций в разработку промышленных ИТ-приложений, исследования в области кибер-безопасности, разработки в области микроэлектроники и цифровых услуг, т.е. в инновации и исследования в национальном масштабе.[37] В соответствии с положениями этого документа, а также для поддержки инноваций в области big data и промышленных, медицинских и исследовательских приложений в Берлине были созданы два больших дата-центра.[38]

В марте 2015 г. правительство Германии опубликовало инвестиционный план поддержки исследований в области кибер-безопасности, который получил название «Самоопределение и безопасность в цифровом мире в 2015-2020 гг.» (Self-Determination and Safety in the Digital World 2015-2020). Этот план предусматривал инвестиции в размере 180 млн. евро (примерно 198 млн. долларов США) на период до 2020 года в разработки новых крипто технологий и дальнейшие разработки

в области защиты персональных данных и коммуникационных услуг. План концентрируется на четырех основных областях: новые технологии, безопасные и надежные информационно-коммуникационные системы, сферы применения технологий кибер-безопасности, а также защита приватности и персональных данных.

Министерство образования и научных исследований (BMBF), которое реализует эти задачи правительства в области исследований и инноваций, создало три центра исследований в области кибер-безопасности в трех университетах: Центр кибер-безопасности, защиты персональных данных и отчетности (Center for IT Security, Privacy and Accountability, CISPA) в Саарбрюккене, Европейский центр разработок в области безопасности и защиты персональных данных (European Center for Security and Privacy by Design, EC-SPRIDE) в Дармштадте и Центр компетенций в прикладных технологиях безопасности (Competence Center for Applied Security Technology, KASTEL) в Карлсруэ. В 2009 г. BMBF и Министерство внутренних дел также согласовали совместную реализацию проекта в области исследований по вопросам кибер-безопасности, создав, таким образом, рабочую программу «Исследования в области кибер-безопасности» (IT Security Research) по созданию и внедрению новых приложений в этой сфере.[39]

Помимо прочего, правительство Германии признает, что для обеспечения устойчивости развития исследований в ИТ сфере следует обеспечить обучение большего количества квалифицированных специалистов. Студенты Центра компетенций KASTEL, финансируемого BMBF, могут получать дипломы специалистов в области кибер-безопасности, эквивалентные степени магистра. Дармштадский технический университет с 2010 года предлагает магистерскую программу в области кибер-безопасности. Специалисты, уже имеющие место работы, могут пройти курсы повышения квалификации по основам кибер-безопасности при Центре прикладных исследований в области кибер-безопасности (CASED) в Дармштадском техническом университете, причем выпускники получают диплом об присвоении степени специалиста в области кибер-безопасности. Факультет компьютерных наук Фрайбургского университета предлагает обучение на степень магистра компьютерных наук с возможностью специализации в области безопасности. Кроме того, эта учебная программа может, по желанию

Правительство Германии признает, что для обеспечения устойчивости развития исследований в ИТ-сфере следует обеспечить обучение большего количества квалифицированных специалистов.

студентов, включать курсы политологии и других общественных наук, что позволит студенту получить более всеобъемлющие знания по вопросам кибер-безопасности и связанных с ними других вопросов.[40]

Кроме прочего, правительство Германии предлагает экономические льготы для проведения корпоративных исследований в трех основных областях: «компьютерные технологии – работа в условиях цифрового мира», «ИКТ – определение и разрешение инцидентов в области кибер-безопасности» и «е-мобильность – новые перспективы для бизнеса». Первые две возможности открыты для компаний из всех секторов экономики, в то время как последняя доступна только компаниям, работающим в области производства и ИКТ. Льготы для стимулирования исследований предусматривают гранты компаниям, консорциумам и исследовательским центрам.[41] Также, недавно немецкое правительство оценило важность венчурных инвестиций в ИКТ сектор, причем с особым упором на ИТ-стартапы. Для того, чтобы оказать содействие росту стартап-движения, правительство также выделяет определенные средства для венчурных инвестиций, в т.ч.: бесплатная информационная и консультационная поддержка основателям стартапов; оптимизация финансирования посредством создания конкурентной рабочей среды и дополнительного инвестирования; привязки стартапов к традиционным компаниям, работающим на подобных сегментах рынка; а также посредством создания международных «стартап центров», в т.ч. и бизнес-инкубаторов.[42]

Германия готовится стать председательствующей страной в Большой двадцатке и принять саммит этой организации в Гамбурге в 2017 г., где у нее будет возможность продемонстрировать свое лидерство в сфере ИТ инноваций и исследований. Гамбургский университет получил финансирование со стороны Европейской комиссии в размере 1 млн. евро (примерно 1,1 млн. долларов США) в 2016 году на финансирование исследовательского проекта в области кибер-безопасности. Гамбургский университет и Независимый центр защиты персональной информации Шлезвиг-Гольштейна (Schleswig-Holstein's Independent Center for Privacy Protection) объединились с девятью другими организациями из семи стран в Исследовательскую сеть Конструктивного альянса за кибер-безопасность как основополагающую ценность (Constructive an Alliance for Value-driven Cybersecurity, CANVAS). Исследователи CANVAS будут вести исследования в области баланса обеспечения высокого уровня кибер-безопасности и соблюдения основополагающих прав человека в трех основных областях: здравоохранение, финансовые системы и национальная безопасность.[43] Тем не менее, в Германии все еще наблюдается серьезный недостаток специалистов в области кибер-безопасности, особенно

в государственных органах страны. Федеральное министерство образования и научных исследований финансирует создание нового института – Германского института интернета (Deutsches Internet Institut, DII) и выделяет 50 млн. евро (примерно 56 млн. долларов США) на его развитие в течение будущих пяти лет. Институт будет вести исследования в сфере этического, экономического, законодательного и представительного аспектов работы интернета и массового перехода к цифровым технологиям в рамках междисциплинарного подхода.[44] Кроме того, Фонд Альберта Эйнштейна (Einstein Foundation) и правительство Берлина заявили о создании Центра цифрового будущего имени Эйнштейна (Einstein Center of Digital Future, ECDF) – нового центра государственно-частного партнерства для исследований развития цифровых технологий в германском обществе. Оба партнера инвестируют 38,5 млн. евро (примерно 43 млн. долларов США) в обучение будущих 50 профессоров в области современных технологий, в т.ч. в вопросах кибер-безопасности.[45] Новый Центр им. Эйнштейна объединит несколько государственных организаций и университетов, в т.ч. Берлинский технический университет, Свободный университет Берлина, Берлинский университет Гумбольдта, Берлинскую высшую школу музыки и Шарите – Университетскую клинику Берлина, а также восемь других известных исследовательских центров и два университета прикладных наук.

6. ДИПЛОМАТИЯ И ТОРГОВЛЯ

Германия в течение нескольких последних лет активно принимала участие в дипломатических, коммерческих и торговых переговорах по проблемам кибер-безопасности. Страна также является одним из ведущих партнеров в рамках инициативы Privacy Shield и других инициатив ЕС, а также подобных проектов между ЕС и США для защиты данных.

В рамках Национальной стратегии кибер-безопасности 2011 года указывается, что «с учетом глобального характера информационно-телекомуникационных технологий, международное сотрудничество… сконцентрированное на аспектах международной политики и безопасности… носит обязательный характер».[46] Действительно, Германия была очень активна в этой области на международной арене, в том числе в рамках сотрудничества в ООН, ЕС, Совете Европы, НАТО, Большой семерке, ОБСЕ и других международных организаций. Тема многостороннего сотрудничества, упомянутая в Национальной стратегии, нашла свое развитие в «Цифровой повестке» 2014-2017 гг. (Digital Agenda 2014-2017), и в настоящее время активно реализуется в рамках работы Германии со следующими организациями:

Международный союз электросвязи (МСЭ), Форум по управлению интернетом (Internet Governance Forum, IGF), Организации экономического сотрудничества и развития (ОЭСР), Группы правительственных экспертов ООН по вопросам экономического сотрудничества в области информации и телекоммуникаций (UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications, GGE). В частности, Германия продемонстрировала большую приверженность международному сотрудничеству и обсуждениям в области ИТ посредством неизменного участия во всех группах правительственных экспертов ООН по этим вопросам.

Кроме того, Германия активно участвует в формальных и неформальных диалогах по вопросам ИКТ с различными партнерами, а также принимает участие в конференциях и обсуждениях по всему миру. «Цифровая повестка» Германии подтверждает растущую зависимость экономики от кибер-безопасности. Так, ФРГ постоянно обращается к вопросам сотрудничества в области развития и участвует в реализации проектов, связанных с расширением кибер-возможностей стран и сообществ, упрочения кибер-безопасности, а также расширением возможностей использования кибер-инструментов в развивающихся странах.

В марте 2016 года США и Германия обязались и«продолжать тесное сотрудничество, в области защиты критически важных элементов инфраструктуры, повышать уровень противодействия кризисным ситуациям и координацию в этой области, а также повышать возможности в этой области третьих стран».[47] В рамках этого Трансатлантического кибер-диалога (Transatlantic Cyber Dialogue) США и Германия также обсуждают недавнее предложение создания внутригерманской системы маршрутизации, вопросы шифрования, а также новые стандарты для электронного оборудования и ПО.

В 2011 г. МИД Германии создал Отдел координации международной кибер-политики (International Cyber Policy Coordination Staff), который ведет работу с другими министерствами и организациями Германии с целью формирования открытого, свободного, безопасного и стабильного киберпространства. Федеральный МИД

МИД Германии создал Отдел координации международной кибер-политики и должности «кибер-послов».

рассматривает международную кибер-политику как комплексное явление, оказывающее влияние практически на все аспекты международной политики. Цели этой политики – использование экономических возможностей, предоставляемых интернетом, а также обеспечение безопасности в киберпространстве.[48] Таким образом, в этой области основными направлениями деятельность МИД ФРГ становятся, среди прочего: соглашение о стандартах разумного управления интернетом, соблюдение международного права, а также разработка мер по укреплению доверия для большей кибер-безопасности. Также, в крупнейших городах Германии были учреждены должности «кибер-послов», которые отвечают за вышеперечисленные направления работы МИД внутри страны.

7. ОБОРОНА И КРИЗИСНОЕ РЕАГИРОВАНИЕ

IВ июле 2016 г. Германское Министерство обороны выпустило новую «Белую книгу по вопросам политики безопасности и будущего Вооруженных сил» (White Paper on German Security Policy and the Future of the Bundeswehr), в которой кибер-риски рассматриваются как одни из важнейших для национальной безопасности.[49] В «Белой книге» также указывается, что «вопросы информатизации приобрели международную стратегическую важность и что их значение продолжает постоянно возрастать».[50] Новая политика правительства ФРГ видит Германию «ключевым игроком» в этих вопросах в Европе и подчеркивает «ответственность страны в области активного формирования глобального порядка в этой области».

В 2016 г. в Германии начался процес становления Командования в кибер- и информационном пространстве

В Белой книге «оборонные аспекты кибер-безопасности всего правительства включены в список приоритетных задач Министерства обороны и Вооруженных сил». Более того, Минобороны также несет ответственность за развитие национального потенциала, в том числе в области «разработки единого подхода и сотрудничества правительства с исследовательскими организациями, бизнесом и другими партнерами».[51] Ключевым компонентом этого плана является наличие серьезной обороны

и военные силы, способные «защитить свободу Германии в киберпространстве».

В апреле 2016 года Германия приступила к процессу создания кибер командования, вслед за тем, как в сентябре 2015 г. министр обороны Урсула фон дер Ляйен объявила о таком намерении.[52] Новая организация, Командование в кибер- и информационном пространстве (Kommando Cyber und Informationsraum, KCIR), объединяет все существовавшие ранее подразделения, работавшие в этой области, а также несет ответственность за кибер-безопасность, ИТ (сетей), военную разведку, системы гео-информирования и позиционирования, а также оперативные коммуникации.[53] Ожидается, что эта структура станет полностью действующей к 1 апреля 2017 г. и ее возглавит офицер в звании генерал-лейтенанта. Планируется, что в состав KCIR войдут 13 500 служащих, которые на момент создания уже служили в других военных и армейских подразделениях. Они будут расквартированы в двух новых центрах – Центре кибер-операций (Cyber operations centre) и Центре кибер-безопасности Вооруженных сил (Bundeswehr cyber security centre).[54] Для армии, как и для любого другого ведомства, составляет проблему найти достаточное количество специалистов, сведущих в вопросах информационных технологий. Тем не менее, командование надеется нанять еще 800 специалистов до конца 2016 года, используя рекламный слоган: «Защита Германии в киберпространстве».[55]

Минобороны Германии также объявило, что оно стремится к тому, чтобы у Вооруженных сил были ресурсы и возможности для нанесения ответного удара в случае необходимости, что позволит новому Кибер-командованию работать на том же уровне, что и другие страны, например – США. Департамент информации и сетевых операций (Department of Information and Computer Network Operations) в рамках Стратегического разведывательного подразделения бундесвера (Bundeswehr's Strategic Reconnaissance Unit) в основном концентрируется на расширении оборонных возможностей. После серьезного анализа законодательства, проведенного в начале XXI века, Минобороны в 2005 году приступило к попыткам разработки наступательных технологий, например, собственных команд хакеров (red teams), отдавая себе отчет в том, что опыт использования такого секретного кибер-вооружения может быть использован исключительно в целях обороны.[56] Министерство обороны также поддерживает контакты с ведущими образовательными учреждениями страны, например – с Европейским колледжем менеджмента и технологий (European School of Management and Technology, ESMT), информируя их о своих требованиях к качеству исследований и обучения специалистов.

Правительство Германии стремится к тому, чтобы оборонные мероприятия не смешивались с разведывательной деятельностью. В 2011 году правительство создало Национальный центр кибер-реагирования в составе Министерства внутренних дел. Этот центр объединяет ресурсы различных правительственных организаций, в том числе – федеральной полиции и службы внешней разведки, а также ресурсы частного бизнеса. Он подотчетен Федеральному офису по информационной безопасности.[57] Изначально в новом центре работали несколько специалистов из МВД, Федеральной службы защиты Конституции и Федеральной службы гражданской обороны и преодоления последствий катастроф. С момента его возникновения Федеральная полиция, Федеральный офис криминальных расследований, Служба внешней разведки, Вооруженные силы и Офис криминальных расследований таможенной службы также предоставили своих экспертов. Национальный совет по кибер-безопасности также несет ответственность за координацию оборонной и кибер-политики. В его составе представлены высокопоставленные военные офицеры.[58]

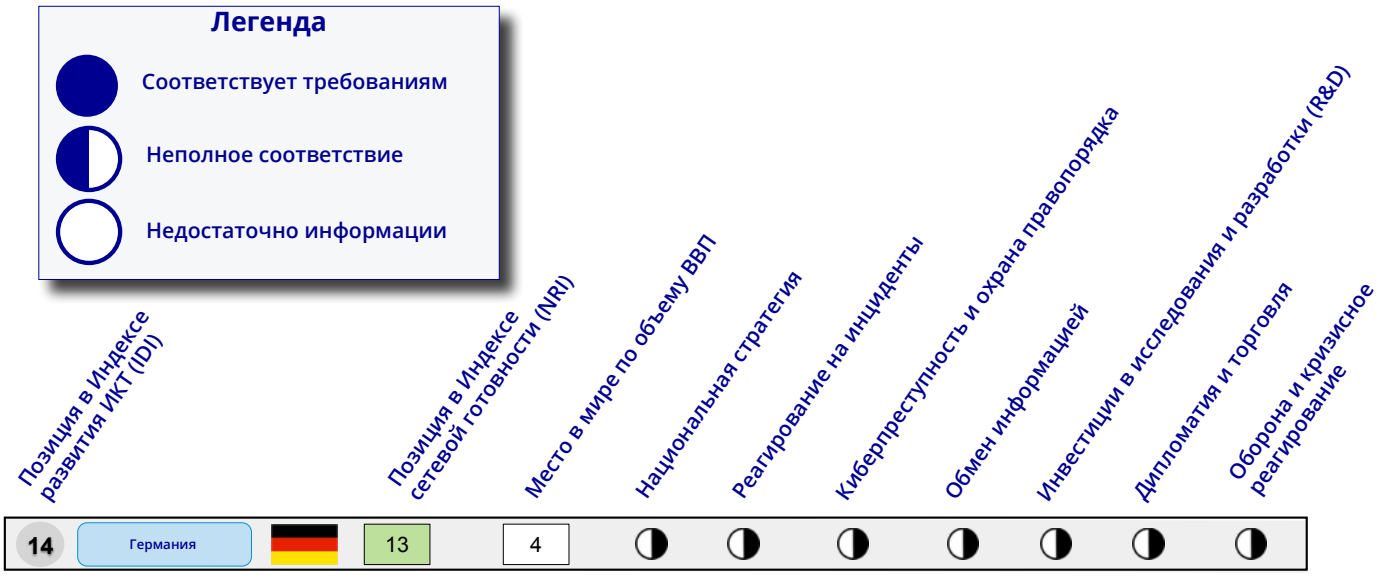
Параллельно со значительным расширением возможностей Минобороны в киберпространстве, правительство предлагает ужесточить контроль за Службой внешней разведки и наложить новые ограничения на ее возможности вести слежку и прослушивание. Эти законодательные реформы, которые еще предстоит обсудить парламенту Германии, запретят Службе внешней разведки вести слежку и прослушивание граждан, государств, органов ЕС, за исключением случаев, когда существуют подозрения о наличие террористической деятельности.[59] Такая реформа также потребует от шефа разведки, офиса федерального Канцлера и независимого судебного совета принять концепцию стратегической внешней разведки на основе списка ключевых слов. Такой подход в корне отличается от подхода других стран, которые напрямую увязывают свои службы разведки со службами обороны.

ЗАКЛЮЧЕНИЕ: ИНДЕКС КИБЕРГОТОВНОСТИ CRI 2.0

По оценке авторов CRI 2.0, Германия находится на пути к полной кибер-готовности и в настоящее время частично соответствует всем требованиям всех семи элементов Индекса

Выводы в рамках настоящего анализа представляют собой отображение динамично меняющегося ландшафта кибер-готовности страны на момент написания отчета. Германия продолжает развивать свои экономическую стратегию и стратегию в области кибер-безопасности, а также политику и инициативы, которые в максимально возможной мере соответствуют национальным приоритетам в области безопасности и экономического развития. Обновления профиля этой страны отразят эти изменения, а также проведут мониторинг и оценку основных и значимых изменений.

Индекс CRI 2.0 предлагает всеобъемлющую экспертную методологию, которая помогает лидерам стран создавать условия для продвижения к более безопасному, более стабильному цифровому будущему в еще более компьютеризированном, конкурентном и конфликтном мире. Чтобы узнать больше об Индексе CRI 2.0, перейдите по ссылке: http://www.potomacinstitute.org/academic-centers/cyber-readiness-index.



БИБЛИОГРАФИЯ

1. Internet Hall of Fame, “Timeline,” http://www.internethalloffame.org/internet-history/timeline.

2. Deutsche Telekom, “Shareholder Structure,” https://www.telekom.com/shareholder-structure.

3. Diann Rusch-Feja and Hans Jurgen Becker, “Global Info: the German Digital Libraries Project,” D-Lib Magazine, vol.5 no. 4 (April 1999), http://www.dlib.org/dlib/april99/04rusch-feja.html.

4. The Federal Government, “Digital Agenda 2014-2017,” (2014): 21, www.digitale-agenda.de/DA/Navigation/DE/Home/home.html.

5. Ibid.

6. Federal Ministry of Economic Affairs and Federal Ministry of Labour and Social Affairs, “IT and Telecommunication,” (2014), http://www.make-it-in-germany.com/en/for-qualified-professionals/working/industry-profiles/it-and-telecommunications.

7. The Federal Government, “2016 White Paper on German Security Policy and the Future of the Bundeswehr,” (July 2016): 22, https://www.bmvg.de/portal/a/bmvg/en/.

8. Ibid.

9. Matthew Karnitschnig, “Why Europe’s Largest Economy Resists new Industrial Revolution,” Politico, July 6, 2016, http://www.politico.eu/article/why-europes-largest-economy-resists-new-industrial-revolution-factories-of-the-future-special-report/.

10. Federal Ministry for Economic Affairs and Energy, “Introducing the German Mittelstand,” http://www.make-it-in-germany.com/en/for-qualified-professionals/working/mittelstand.

11. Sara Zaske, “Germany’s vision for Industrie 4.0: The Revolution will be digitized,” ZDNet, February 23, 2015, http://www.zdnet.com/article/germanys-vision-for-industrie-4-0-the-revolution-will-be-digitised/.

12. “Two in Five Internet Users in Germany Hit by Cybercrime in 2013,” eMarketer, May 21, 2014, http://www.emarketer.com/Article/Two-Five-Internet-Users-Germany-Hit-by-Cybercrime-2013/1010845.

13. “Merkel: ‘Difficulties Yet to Overcome’ in US Spy Scandal,” CBS DC, May 2, 2014, http://washington.cbslocal.com/2014/05/02/merkel-difficulties-yet-to-overcome-in-us-spy-scandal/.

14. Melissa Hathaway's interview with Dr. Sandro Gaycken, Director of the Digital Society Institute, ESMT Berlin, September 20, 2016.

15. Federal Ministry of the Interior, "Cyber Security Strategy for Germany," (2011), https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile.

16. Flippa von Stackelberg, "Germany Prepares for Cyber War," New Security Learning, http://www.newsecuritylearning.com/index.php/feature/88-germany-prepares-for-a-cyber-war

17. Federal Ministry of the Interior, "Cyber Security Strategy for Germany."

18. The new National Cyber Response Centre pools the cyber defense resources of the Federal Office for Information Security, the Federal Office for the Protection of the Constitution, the Federal Intelligence Service, the Federal Police, the Customs Criminal Investigation Office, the German Military, the Federal Office of Civil Protection and Disaster Assistance, and the Federal Criminal Police Office; and it will cooperate with ISPs.

19. TÜViT, "Alliance for Cyber Security," https://www.tuvit.de/en/cyber-security/alliance-for-cyber-security-2352.htm.

20. Federal Government, "Digital Agenda 2014-2017," 5.

21. Federal Office for Information Security, "The State of IT Security in Germany 2015," (2015): 42, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2015.pdf?__blob=publicationFile&v=2.

22. Federal Office for Information Security, "Annual Report," (2003): 27, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/annualreport/BSI-AnnualReport2003_pdf.pdf?__blob=publicationFile.

23. Melissa Hathaway's Interview with Arne Schonbohm, Director of BSI, June 8, 2016, in Berlin, Germany.

24. Federal Office of Information Security, "CERT-Bund," https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/Cert-Bund/cert-bund_node.html.

25. Bürger CERT, "About Us," https://www.buerger-cert.de/about.

26. Federal Ministry of the Interior, "National Plan for Information Infrastructure Protection," (2009), http://www.qcert.org/sites/default/files/public/documents/GER-PL-National%20Plan%20For%20Information%20Infrastructure%20Protection-Eng-2005.pdf, and "CIP Implementation Plan for Information Infrastructure Protection," (2007) http://www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/2009/kritis.html.

27. Federal Ministry of the Interior, "CIP Implementation Plan for Information Infrastructure Protection."

28. Federal Ministry of the Interior, "Cyber Security Strategy for Germany."

29. Melissa Hathaway, "Best Practices in Computer Network Defense: Incident Detection and Response," NATO Science for Peace and Security Series, Information and Communications Security, vol.35, (IOS Press, February 2014): 12, http://www.iospress.nl/book/best-practices-in-computer-network-defense-incident-detection-and-response/.

30. Joe Uchill, "German Intelligence Blames Russia, China for Cyberattacks," The Hill, June 28, 2016, http://thehill.com/policy/cybersecurity/285202-german-intelligence-blames-russia-china-for-cyber-attacks?utm_source=&utm_medium=email&utm_campaign=2679.

31. Watson Farley & Williams, "Briefing: The New German IT Security Act," February 2016, http://www.wfw.com/wp-content/uploads/2016/02/WFW-Briefing-Germany-IT-Security-Feb-2016-EN-15-Feb.pdf.

32. Federal Ministry of Justice and Consumer Protection, (2015), http://www.gesetze-im-internet.de/englisch_stgb/index.html.

33. Center for Strategic and International Studies, "Cybersecurity and Cyberwarfare," (2011), http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf.

34. Federal Ministry of the Interior, "Cyber Security Strategy for Germany," 10.

35. US Department of State, "Joint Statement on US-Germany Cyber Bilateral Meeting," June 27, 2014, http://www.state.gov/r/pa/prs/ps/2014/06/228543.htm.

36. National Cyber-Forensics & Training Alliance, "Become a NCFTA Partner," https://www.ncfta.net.

37. Federal Government, "Digital Agenda 2014-2017."

38. Federal Ministry of Education and Research, "Berlin Big Data Center," http://www.bbdc.berlin/start/.

39. Federal Ministry of the Interior, "Cyber Security Strategy for Germany," (2011): 11, and Federal Ministry of Education and Research, "Digital World: Cybersecurity research to boost Germany's competitiveness," https://www.bmbf.de/en/cybersecurity-research-to-boost-germany-s-competitiveness-1418.html.

40. University of Freiburg, "Department of Computer Science," http://www.informatik.uni-freiburg.de/studies/studies.

41. Deloitte, "Grants and Incentive Program Updates: The Latest Legislative Developments From Around the world," (April 2015), https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/tax/deloitte-nl-tax-grants-and-incentives-newsletter-april-2015.pdf, and Deloitte, "2014 Global Survey of R&D Tax Incentives," (March 2014): 17, http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Tax/dttl-tax-global-rd-survey-aug-2014.pdf.

42. OECD, "OECD Digital Economy Outlook 2015," (July 15, 2015): 25, http://www.oecd.org/internet/oecd-digital-economy-outlook-2015-9789264232440-en.htm.

43. "1 Million Euro for Cyber Security Project at Hamburg University," Hamburg News, June 21, 2016, http://www.hamburg-news.hamburg/en/cluster/media-it/eu-funds-research-project-ethical-cyberspace/.

44. Georg Schütte, State Secretary at the Federal Ministry of Education and Research, "New Year's Reception for the Science Counsellors of the Foreign Embassies," January 25, 2016, https://www.bmbf.de/de/the-ccasion-of-the-new-year-s-reception-for-the-science-counsellors-of-the-foreign-2381.html.

45. Melissa Hathaway's interview with Professor Philip Lark, September 26, 2016. For more information on the Einstein Center of Digital Future (ECDF), see: http://be-digital.berlin/the-einstein-center-digital-future/.

46. Federal Ministry of the Interior, "Cyber Security Strategy for Germany."

47. US Department of State, "Joint Statement on U.S.-Germany Cyber Bilateral Meeting," March 24, 2016, http://www.state.gov/r/pa/prs/ps/2016/03/255082.htm.

48. Federal Foreign Office, "International Cyber Policy," http://www.auswaertiges-amt.de/EN/Aussenpolitik/GlobaleFragen/Cyber-Aussenpolitik/KS-Cyber-Aussenpolitik_node.html.

49. The Federal Government, "2016 White Paper on German Security Policy and the Future of the Bundeswehr." Germany's Defense White Papers are released periodically; the previous one was released in 2011.

50. Ibid, 37.

51. Ibid, 93.

52. Federal Ministry of Defense, "Keynote Address by Minister von der Leyen at Cyber-Workshop," September 17, 2015, https://www.bmvg.de/portal/a/bmvg/!ut/p/c4/NYy7CsJAEEX_aCYrgmCXkBSCjTYaG9nsDnFgH-2GcrI0fb7bwHjjNgYsP3Ei28GyVc7IB-7zg6Pk4fmGKZIa5BOZJnC4U9ZSvuxQU-80zNy4reScMJbffEELifSaqWkvHkWq1lg-yaKhllVkK8Aex8b0XWOa_8y33Q3D5W-wO-_7UXXGJsf0B62YR2w!!/.

53. До этого момента Вооруженые силы Германии, как и другие современные армии, разделяли свои оперативные отделы и отделы по операциям в сфере ИТ. Новая команда объединяет два вида командований по примеру американской модели организационной структуры, используемой в Кибер-командовании Флота США /C10F. Скорость работы новой организации и ее инновационная структура являются крайне необычной практикой для германского министерства обороны, а также свидетельством серьезных намерений Правительства как защищать свою страну, так и увеличить ее влияние на решение важнейших международных ИТ-проблем.

54. Federal Ministry of Defense, "Final Report: Building the Cyber and Information Space Command," https://www.bmvg.de/portal/a/bmvg/!ut/p/c4/NYyxDsIwDAX_yE4WRNladYENpArKljZRsRQnlXHCwsfTDryTbjnp4RM-3kqu0OKWcXMQHjjOdpg9MXBf-gEpU4eHJQyYfsZH5RBaZEbw1Ch-fG-X_gAc05Bd2tlSpsXcZoF1iwa91JEt-gLkcTS274w1_9lv2_SX4Xo4Nv25u-HK-3P4AaMgbvg!!/.

55. Christoph Hickmann, "Call to Arms for Cyber War, Trying to Poach Private Sector Recruits," Süddeutsche Zeitung, April 18, 2016, http://international.sueddeutsche.de/post/143005903195/call-to-arms-for-cyber-war-trying-to-poach.

56. "Germany Reveals Offensive Cyberwarfare Capability," Atlantic Council, June 8, 2012, http://www.atlanticcouncil.org/blogs/natosource/germany-reveals-offensive-cyberwarfare-capability.

57. James Lewis and Katrina Timlin, "Cybersecurity and Cyberwarfare," Center for Strategic and International Studies, (2011): 12-13, http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf.

58. Federal Ministry of the Interior, "Cyber Security Strategy for Germany," 8-10.

59. Thorsten Severin and Andrea Shalal, "German Government Agrees to Reform BND Spy Agency – Sources," Reuters, June 3, 2016, http://af.reuters.com/article/worldNews/idAFKCN0YP2KG.

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 при колледже Кеннеди в Гарвардском университете. Работала с двумя президентскими администрациями США, в том числе 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 киберготовности. Регулярно публикует исследовательские статьи по вопросам кибербезопасности относящимся к государственным и корпоративным интересам. Статьи доступны по адресу: http://belfercenter.ksg.harvard.edu/ experts/2132/melissa_hathaway.html.

Крис Демчак (Chris Demchak) - эксперт проекта Индекс киберготовности Потомакского института политических исследований. Сферами ее научного интереса являются: киберустойчивость, киберконфликты, 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. Является автором книги «Войны на устойчивость и разрушение: киберконфликты, власть и национальная безопасность»

Джейсон Кербен (Jason Kerben) - эксперт проекта «Индекс киберготовности» 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 киберрисками и консультирует по множеству отдельных видов деятельности, различным образом связанных с кибербезопасностью, в том числе по международным принципам в области ИКТ, управлению системами допуска, текущей диагностики систем, а также киберстрахованию.

Дженнифер МакАрдл (Jennifer McArdle) – внештатный научный сотрудник Потомакского института политических исследований и доцент-профессор по кибербезопасности в университете Salve Regina, в Ньюпорт. В сферу ее научных интересов входят кибер-конфликты, управление эскалации конфликтов и военные разработки. Она заканчивает диссертацию на соискание звания Доктора философии в Королевском колледже, Лондон, на отделении изучения войн и военного дела.

Франческа Спидальери (Francesca Spidalieri) - эксперт проекта «Индекс киберготовности» Потомакского института политических исследований. Также является старшим научным сотрудником по киберлидерству в Пелл-центре, университет Salve Regina, и Заслуженным научным сотрудником в Институте Понемон . Сфера научных интересов: развитие киберлидерства, управление киберрисками, киберобразование, а также обучение специалистов в области кибербезопасности. Недавно опубликовала отчет «Положение дел в кибербезопасности в Штатах», содержащий оценки киберготовности разных штатов США в соответствии с данными ИКГ 1.0.

Для получения общей информации или для участия в проекте CRI 2.0, обращайтесь по адресу:

CyberReadinessIndex2.0@potomacinstitute.org

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