КИБЕРГОТОВНОСТЬ ФРАНЦИИ: КРАТКАЯ ИНФОРМАЦИЯ

Ведущий исследователь: Мелисса Хатауэй

Крис Демчак, Джейсон Кербен, Дженнифер МакАрдл, Франческа Спидальери

Сентябрь 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

Благодарность:

Потомакский Институт политических исследований и авторы доклада хотели бы поблагодарить следующих людей за их вклад: г-жу Валери Деруэ-Мазойе, координатора Стратегического комитета французской атомной промышленности (CSFN) и Старшего вице-президента, подотчетного Старшему исполнительному вице-президенту по вопросам ядерной энергетики EDF Группы; г-жу Фредерик Дузе (PhD), Председателя Кастекс кафедры киберстратегии и профессора Французского института геополитики, Университета Париж 8. Авторы хотели бы также поблагодарить Алекса Талиесина за графическое оформление 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.

КИБЕР-ГОТОВНОСТЬ ФРАНЦИИ: КРАТКАЯ ИНФОРМАЦИЯ

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 2

1. НАЦИОНАЛЬНАЯ СТРАТЕГИЯ. 7

2. РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ 10

3. КИБЕРПРЕСТУПНОСТЬ И ОХРАНА ПРАВОПОРЯДКА . . . 13

4. ОБМЕН ИНФОРМАЦИЕЙ 15

5. ИНВЕСТИЦИИ В ИССЛЕДОВАНИЯ И РАЗРАБОТКИ (R&D) 16

6. ДИПЛОМАТИЯ И ТОРГОВЛЯ 19

7. ОБОРОНА И КРИЗИСНОЕ РЕАГИРОВАНИЕ. 21

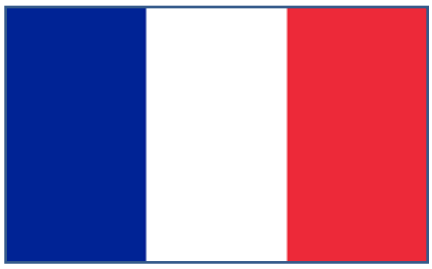
ЗАКЛЮЧЕНИЕ: ИНДЕКС КИБЕРГОТОВНОСТИ CRI 2.0 26

БИБЛИОГРАФИЯ 27

ОБ АВТОРАХ 34

КИБЕРГОТОВНОСТЬ ГЕРМАНИИ

КРАТКИЙ ОБЗОР



Население	66,6 миллионов
Прирост населения	0,5%
ВВП в рыночных ценах (по текущему курсу доллара США)	$2,422 трлн.
Рост ВВП	1,2%
Год появления Интернета	1981
Год принятия Национальной стратегии кибер-безопасности	2011, 2015
Национальные доменные зоны	.fr
Количество пользователей фиксированного широкополосного доступа на 100 пользователей интернета	40,2
Количество контрактов на мобильный широкополосный доступ на 100 пользователей интернета	66,2
Количество мобильных номеров на 100 пользователей	100,4

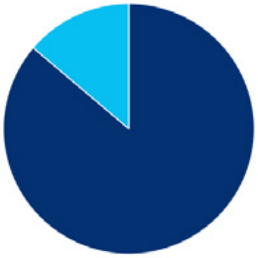
Развитие Информационно-коммуникационных технологий (ИКТ) и степень развития коммуникаций в стране

Позиция в Индексе развития ИКТ (IDI) Международного союза электросвязи (МСЭ)	17	Индекс сетевой готовности (NRI) Всемирного экономического форума	26

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

ВВЕДЕНИЕ

В 1981 году французской общественности был представлен предшественник интернета - видеотекстовая онлайн служба «Minitel», выведенная на рынок на тот момент государственной компанией France Telecom (вернее ее предшественником - Postes, Télégraphes et Téléphones, PTT), которая была упразднена в 2012. Поскольку эта услуга была преимущественно текстовой, она была бесплатной для граждан Франции, равно как и базовое оборудование для ее использования. Пользователи могли пользоваться чатами, совершать онлайн-бронирование и покупки, банковские операции и поиск в базах телефонных номеров. Проект носил одновременно технический и политический характер, имея целью обеспечить цифровое будущее и технологическую независимость Франции и ее общества.[1] Программа финансировалась из государственного бюджета и реализовывалась согласно Французской индустриальной политике, принятой в конце 1940-х годов, которая рассматривала инвестиции в телекоммуникационные технологии как ключевой элемент экономического развития.[2]
Служба «Minitel» стала терять свою значимость с появлением глобальной сети интернет в 1990-е годы. На сегодняшний день Франция – страна с одним из самых высоких уровней использования интернета в Европе (более 83%), что выше среднего уровня по ЕС (79%).[3] По состоянию на 2011 г., примерно четверть экономического роста Франции связана с развитием в сфере ИКТ, что соответствует целям Французской индустриальной политики 1940-х годов.[4]



Уровень использования интернета во Франции: 83.8%

В 2011 году, после публикации Стратегии цифрового равития, получившей название Plan France Numérique 2012-2020: Bilan et Perspectives, правительство Франции удвоило свои усилия по поддержке использования информационно-коммуникационных технологий (ИКТ) в национальном масштабе, особенно в виде механизма создания новых рабочих мест и стимулирования роста (уровень безработицы в стране составляет примерно 11% для всего трудоспособного населения и 25% для молодежи). В 2012 году правительство Франции запустило первый в ЕС проект по созданию акционерного венчурного фонда по развитию цифровой инфраструктуры с целью предоставления высокоскоростного широкополосного (беспроводного) доступа в интернет для сельских районов Франции, с целью обеспечить лучшее распределение экономического развития по всей территории страны.[5]
В 2013 г. была начата реализация национального плана, стимулирующего предоставление доступа к максимально

высокоскоростному доступу в интернет для каждого домохозяйства к 2025 году, с использованием наиболее подходящих для каждого отдельного региона технологий. Фиксированный широкополосный доступ (по кабельным или телефонным сетям) доступен на всей территории страны и продолжает активно развиваться.[6] Кроме прочего, ИКТ сектор обеспечивает 3,7% рабочих мест во французской экономике, 5,2% ВВП страны и 7,9% от всей производимой частным сектором добавочной стоимости. По оценкам специалистов, в 2014-2015 гг. в ИКТ-секторе было создано более 450000 рабочих мест и создано 130 млрд. евро (примерно 148,6 млрд. долларов США) добавочной стоимости.[7] Стратегия цифрового равития продолжает давнюю тенденцию правительства Франции делать значительный упор на развитие телекоммуникационного сектора (сейчас - ИКТ в целом) как основного средства построения конкурентоспособной экономики с возможностью трудоустройства для всех (особенно - для молодежи), а также для поддержания социальных ценностей Франции.[8]

Стратегия определяет 57 целевых показателей для развития экономики Франции к 2020 году. Таким образом, правительство стремится достигнуть следующих целей: роста объема цифровых технологий в работе каждой компании страны, преобразования всех наземных телекоммуникационных каналов с использованием технологий высокого разрешения, а также переход к безбумажному документообороту для всех государственных органов к 2020 г. Наряду со Стратегией цифрового равития, Франция также начала реализацию национальной программы инвестиций в ИКТ сектор, в рамках которой выделяется 2 млрд евро (примерно 2,3 млрд долларов США) на развитие интернет-инфраструктуры в стране (т.е. высокоскоростного мобильного доступа в интернет, оптоволоконной связи, а также спутниковых цифровых каналов связи) в период до 2025 года.; 2,25 млрд евро (примерно 2,5 млрд долларов США) для поддержки развития инновационных цифровых услуг, контента и приложений; а также 250 млн. евро (примерно 282 млн. долларов США) на развитие современных «умных» сетей. Помимо этого, в 2012 году французское правительство приступило к реализации программы «Большой Париж», в рамках которой столица станет современным центром цифровой экономики, привлекающим компании, специалистов и инвестиции со всего мира.[9] Наконец, Банк общественных инвестиций (Public Investment Bank, BPI) недавно дал старт инициативе, получившей название «Фонд цифровых амбиций BPI» (Digital Ambition Fund of BPI) с целью поддержки развития стартапов, связанных с интернет-услугами и новыми бизнес-моделями, ассоциирующимися с интернетом вещей. Среди других интересов инициативы – цепочки блоков транзакций, или блокчейн (blockchain) и облачные технологии, автомобили с доступом в интернет, цифровой маркетинг, кибер-безопасность и другие

цифровые продукты и услуги, которые продвигают инновационные бизнес-модели. Банк заявил, что планирует на первоначальном этапе инвестировать суммы от 1 до 10 млн евро (от 1,1 до 11,2 млн долларов США).[10]

Параллельно с этими цифровыми экономическими инициативами, Франция также приняла четыре политических документа, акцентирующих внимание на то, как кибер-незащищенность затрагивает французскую экономику и безопасность. Отчет Сената Франции от 2012 года характеризовал национальные кибер-потери как «систематическое разграбление дипломатического, культурного и экономического наследия Франции».[11] В пакет центральных политических документов, всесторонне определяющих национальную стратегию кибер-безопасности, входят: 1) «Белая книга по вопросам национальной обороны и безопасности» 2008 г.; 2) «Кибер-стратегия Франции» 2011 г.; 3) «Белая книга по вопросам национальной обороны и безопасности» 2013 г.; и 4) «Национальная стратегия цифровой безопасности Франции» 2015 г.[12] Текст последнего документа был официально представлен Премьер-министром Мануэлем Вальсом и характеризуется как инструмент поддержки цифровой трансформации французского общества. Как отметил г-н Вальс в ходе презентации, «поддерживая развитие цифрового общества, мы также поддерживаем создание киберпространства, которое обеспечит нам устойчивую платформу для роста и будущих возможностей для французских компаний, таким образом поддерживая наши демократические ценности и охраняя цифровые данные и приватность наших граждан».[13] Французское правительство напрямую увязывает свое благосостояние с кибер-безопасностью страны. Так, три недавних события ярко продемонстрировали, каким образом киберпространство может использоваться террористическими группами для планирования и координации действий в ходе терактов, а СМИ, в свою очередь, для оперативного информирования мировой общественности об этих терактах, и, наконец, властями для обнаружения виновников. Сатирический еженедельник «Шарли Эбдо» стал жертвой атаки террористов в январе 2015 г. после публикации контента, который мог показаться оскорбительным для верующих. В ноябре 2015 года в Париже в шести общественных местах произошли теракты, в том числе – в ночном клубе и на стадионе. В ходе расследования выяснилось, что нападающие использовали для общения шифрованные коммуникаторы WhatsApp и Telegram.[14] Последний теракт, в День взятия Бастилии в июле 2016 г. в Ницце, привел к продлению Президентом Олландом режима чрезвычайного положения, который позволяет органам безопасности

применять исключительные меры, такие как обыски и задержания, а также более свободно контролировать использование интернета.[15] Кроме того, французское правительство провело ряд заседаний в закрытом режиме с участием представителей компаний управляющих социальными сетями и поисковыми сервисами. Правительство попросило их более тесно сотрудничать с властями для немедленного удаления экстремистской пропаганды по требованию властей. [16] Для того, чтобы оказывать более качественные услуги своим гражданам, в июне 2016 года правительство Франции выпустило приложение для смартфонов, которое первоначально предназначалось для информирования болельщиков Евро-2016 о возможных терактах, однако в настоящее время и далее правительство планирует использовать это приложение для информирования о потенциальных рисках. [17]

Кибер-безопасность являлась приоритетным направлением деятельности даже до совершения терактов 2015-2016 гг. В 2001 году правительство Франции преобразовало информационную службу безопасности правительства в Центральный отдел безопасности информационных систем (Central Information Systems Security Division, DCSSI) под руководством Генерального секретаря Национальной обороны, чтобы координировать кибер-защиту национальной инфраструктуры и электронных систем правительства. В 2009 году этот орган был преобразован в Национальное агентство безопасности информационных систем (Agence Nationale la Sécurité des Systèmes d'Information, ANSSI), которое в 2011 году подготовило первую французскую стратегию кибер-безопасности. В том же году ANSSI стало органом, ответственным за оборону информационных систем общегосударственного значения, в том числе за руководство защитными мерами, а иногда и по регулированию значимых промышленных систем и корпораций страны. Обеспечение национальной кибер-безопасности облегчается высокой централизацией власти во Франции в сферах экономики и национальной безопасности. «Белая книга по вопросам национальной обороны и безопасности» 2013 г. подчеркивает, что для обеспечения безопасности в киберпространстве необходимы дополнительные усилия, а также что необходимым элементом оборонной кибер-стратегии Франции должна являться разработка наступательных кибер-возможностей.[18] Принятием решения о создании команды кибер-реагирования сразу после возникновения ANSSI, правительство Франции продемонстрировало наличие у него комплексного подхода к проблеме устранения кибер-угроз и учета приоритетов национальной безопасности в своей экономической политике.

Для оценки готовности Франции к преодолению кибер-рисков использовался Индекс кибер-готовности (CRI) 2.0. Приведенный ниже анализ содержит базовые исходные данные, которые позволят Франции 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, киберпреступность и охрана правопорядка, обмен информацией, инвестиции в исследования и разработки, дипломатия и торговля, а также оборона и кризисное реагирование):

Оценка кибер-готовности Франции (2016)

1. НАЦИОНАЛЬНАЯ СТРАТЕГИЯ

В течение последних нескольких лет Франция полностью переформатировала свои приоритеты в области обороны и национальной безопасности, учитывая увеличение объема, уровня, интенсивности и сложности национальных кибер-угроз, в том числе кибер-преступности, политического и экономического шпионажа, нападений на важнейшие объекты инфраструктуры, а также других кибер-нарушений. «Белая книга по вопросам национальной обороны и безопасности» 2008 г. являлась первым основополагающим документом, адресованным исключительно проблематике национальных кибер-угроз как основному риску для национальной безопасности и суверенитета. В ней определялись новые приоритеты, такие как предотвращение и реагирование на кибер-атаки, а также предусматривались институциональные изменения, необходимые для обеспечения национальной безопасности.[19] В соответствии с рекомендациями «Белой книги» 2008 г., один из трех органов, напрямую подчиненных Премьер-министру, - Генеральный секретариат национальной обороны (Secrétariat Général de la Défense Nationale, SGDN) был переименован в Генеральный секретариат обороны и национальной безопасности (Secrétariat Général de la Défense et de la Sécurité Nationale, SGDSN). Эти перемены привели к расширению полномочий Секретариата – от обеспечения классической обороны с использованием Вооруженных сил – к более широким обязанностям обеспечения безопасности всего общества в случаях, выходящих за рамки необходимости использования только военных сил или традиционных агентств безопасности. Эти более широкие полномочия стали отражением необходимости обеспечить защиту общества в новые, более сложные и неспокойные времена, особенно с учетом все более высокой вероятности совершения кибер-преступлений со стороны неприятельских государственных или внесистемных противников. В 2009 г. Главное управление компьютерной безопасности

Национальное агентство безопасности информационных систем (ANSSI), было создано в 2009 г. и является органом, ответственным за безопасность национальных информационных систем.

(DCSSI) было преобразовано в Национальное агентство безопасности информационных систем (Agence Nationale la Sécurité des Systèmes d'Information, ANSSI), и теперь является органом, ответственным за безопасность национальных информационных систем. [20] Концентрируя усилия на решении проблемы роста вероятности новых кибер-атак в отношении страны, ANSSI служит также межведомственным органом под прямым руководством Премьер-министра, ответственным за координацию деятельности по обеспечению кибер-безопасности в национальном масштабе для ключевых предприятий и государственных органов, включая Вооруженные силы. [21] С 2011 г. ANSSI является также национальным органом, несущим ответственность за оборону информационных систем и сетей как в государственном, так и в частном секторах.[22]

Первая Национальная кибер-стратегия Франции была опубликована в 2011 г., а ее вторая версия – в 2015 г.

Вслед за созданием этого органа, в 2011 г. во Франции была опубликована первая национальная кибер-стратегия: «Оборона и безопасность информационных систем: стратегия Франции».[23] Эта стратегия содержит четыре основные цели: обеспечение мирового лидерства в вопросах кибер-обороны, охрана аппарата принятия решений во Франции посредством защиты суверенной информации, повышение уровня кибер-безопасности критически-важных элементов инфраструктуры, а также обеспечение безопасности в кибер-пространстве. «Белая книга по вопросам национальной обороны и безопасности» 2013 г. являлась исправленной версией этого документа от 2008 г. и делала особый упор на угрозе кибер-саботажа в отношении критически важных элементов инфраструктуры.[24]

В 2015 году правительство Франции опубликовало вторую национальную стратегию кибер-безопасности – «Национальную стратегию цифровой безопасности Франции», как свою реакцию на рост количества и серьезности кибер-атак в самых различных сферах.[25] Основанная на предыдущих документах в области безопасности, а также опыте в реализации предыдущей цифровой стратегии, новая стратегия 2015 года объявляет о намерении превратить Францию в «цифровую республику», признавая, что ИКТ –

одновременно является как источником экономического роста и инноваций, так и источником повышенных кибер-рисков.[26] Новая стратегия призывает правительство создать средства для защиты основополагающих интересов Франции в киберпространстве, защиты национальных информационных систем, а также критически важных элементов инфраструктуры. В целом, стратегия кибер-безопасности Франции содержит пять ключевых целей на пути создания «цифровой республики», с одновременным обеспечением безопасности и гибкости ИКТ систем. Эти пять стратегических приоритетов включают: 1) защиту основополагающих интересов Франции в кибер-пространстве - таких как государственные информационные системы и критически важные элементы инфраструктуры; 2) обеспечение взаимного доверия, приватности и защиты персональных данных в сети посредством разработки продуктов для кибер-безопасности, а также предоставления юридической и технической помощи в этой области; 3) повышение осведомленности в вопросах кибер-безопасности и рост потенциала в этой области в национальном масштабе; 4) развитие благоприятной атмосферы для развития предпринимательской деятельности, инвестиций в ИКТ и инновационного бизнеса; и 5) разработка «дорожной карты» для достижения европейской стратегической цифровой автономии.

Стратегия кибер-безопасности Франции 2015 г. является оперативным продолжением «цифровой стратегии» 2011 г., а многие меры кибер-безопасности, перечисленные в «цифровой стратегии», повторяются в Стратегии кибер-безопасности. Так, оба документа предусматривают повышение уровня взаимного доверия в сети, поддержание высокого уровня исследований и разработки инструментов кибер-безопасности как источника экономического роста, а также обеспечение безопасности персональных данных. Что еще более важно, в обоих документах признается, что ИКТ – один из ведущих источников экономического роста Франции, но также и то, что ИКТ системы должны быть надежными и безопасными, и что только в таком случае страна может в полной мере воспользоваться преимуществами роста на основе развития ИКТ. Несмотря на то, что на реализацию последней стратегии не выделялись средства, на обеспечение кибер-безопасности ранее были выделены фонды в размере 1 млрд. евро (примерно 1,1 млрд долларов США). То, что документ был презентован Премьер-министром Вальсом, сигнализирует о том, что французское правительство действительно придает большую важность вопросам кибербезопасности.[27]

2. РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ

Франция создала первую Команду компьютерного реагирования (CERT-FR) в 2000 г, и в ее задачи входил сбор данных и содействие в области реагирования на инциденты

Параллельно с исполнением обязанностей национального органа, обеспечивающего безопасность информационных сетей, ANSSI также исполняет роль организации, ответственной за реагирование на кибер инциденты, «которые непосредственно касаются жизненно важных для страны организаций или операторов», а также за координацию таких действий, предпринимаемых правительством, бизнесом и международными организациями.[28] Будучи ведущим игроком, обеспечивающим кибер-безопасность для Франции, ANSSI действует в качестве правительственной Компьютерной группы реагирования на чрезвычайные ситуации (CERT), которая также предоставляет рекомендации и советы в области защиты и устойчивости общественных сетей и важнейших элементов инфраструктуры, проводит аудит секретной правительственной инфраструктуры информационной безопасности, а также обучает правительственных специалистов. ANSSI на своем сайте регулярно публикует и обновляет информацию по вопросам кибер-безопасности, рекомендации и примеры из практики для государственных органов, компаний любых размеров и рядовых граждан.

ANSSI также является материнской организацией для Оперативного центра безопасности информационных систем (Centre Opérationnel de la Sécurité des Systemes d'Information, COSSI), который является государственной организацией, несущей исключительную ответственность за определение и предотвращение кибер-атак против государственных информационных систем. В 2000 году французское правительство создало первую национальную команду компьютерного реагирования (CERT), которая стала частью COSSI, и в чьи обязанности входила агрегация всех необходимых данных, а также обеспечение содействия жертвам в случае кибер-инцидентов.[29] Изначально получившая название CERTA, эта организация в 2014 году была переименована в CERT-FR. Являясь подразделением ANSSI как часть COSSI, CERT-FR предоставляет поддержку в случаях инцидентов в круглосуточном режиме включая праздники и выходные, а также служит международным контактным узлом по вопросам всех кибер-инцидентов, так или иначе затрагивающих Францию.

В частности, эта команда проводит анализ выявленных уязвимостей и вредоносных кодов; проводит мониторинг регионов страны на предмет возможных инцидентов; координирует меры реагирования на инциденты как со стороны правительства, так и операторов критически важных элементов инфраструктуры; рассылает оповещения и информацию об инцидентах национального масштаба; а также предлагает специальную систему информирования на основе электронной почты для ведения логов таких инцидентов.

Во Франции принят консолидированный межведомственный план реагирования на инциденты под названием "Vigipirate", а один из 12 аспектов этого плана – инциденты в области кибер-безопасности, описывается специальным планом - "Plan Piranet". [30] Этот план разработан для противодействия атакам, которые ставят своей целью нанести серьезный ущерб жизненно важным интересам страны, ее населению, имуществу, окружающей среде или жизненно важной деятельности французских организаций. Такой уровень атаки, по определению ANSSI, определяется следующими признаками: наличием действий, ведущих к блокировке или параличу сетей или систем (например, распределенные DoS-атаки); широкомасштабным заражением устройств вредоносным ПО или целенаправленным повреждением целостности информационных систем (т.е. вирусы, вредоносное ПО и т.п.); а также, в широком смысле, любыми действиями, направленными на повреждение или разрушение информационных систем (т.е. захват, саботаж и т.п.).

В «Белой книге по вопросам национальной обороны и безопасности» 2013 года Франция объявила о необходимости «упреждающего ИТ-потенциала, связанного с возможностями разведки», чтобы расширить возможности реагирования, доступные правительству. Такой подход позволяет предпринимать действия, «различной степени сложности с более-менее обратимыми последствиями, в зависимости от масштаба и серьезности атак». [31] Как и «Белая книга» 2008 г., новая версия сделала особый упор на том, что механизмы определения и защиты от кибер-атак и механизмы защиты конфиденциальных информационных систем являются «важнейшей частью национального суверенитета Франции» и ее экономического благосостояния. Документ содержит намерения увеличить финансирование и выделить больше человеческих ресурсов для реализации этих задач, одновременно указывая, что правительство Франции посредством законодательных и регулятивных действий, определит особые стандарты безопасности для всех операторов критически важных элементов инфраструктуры (Opérateurs d'Importance Vitale, OIV), а также других важных систем как в государственном, так и в частном секторе. Такие стандарты будут основаны в наибольшей степени на аудите, проверке качества

информационных систем организаций, управлении системами оповещения об инцидентах, а также использовании возможностей ANSSI и, при необходимости, других государственных органов, для предотвращения наступления кризисов национального масштаба.

Кроме того, Министерство обороны, в сотрудничестве с ANSSI разрабатывает Резервные силы кибер-защиты (RCD), в которые войдут 4000 гражданских лиц, подготовленных на случай крупного кризиса на всей территории страны. Кроме того, к 2017 году планируется запустить цифровую платформу, на основе которой будет оказываться содействие жертвам атак в государственно-частном партнерстве, в частном секторе, а также рядовым гражданам.[32]

Поскольку правительство Франции несет верховную ответственность за безопасность операторов критически важных элементов инфраструктуры (OIVs), Закон о военном планировании 2013 г. (Loi de Programmation Militaire 2014-2019, LPM) также содержит четыре специальных меры безопасности, применимые к государственным сетям и сетям частных операторов критически важной инфраструктуры.[33] На основе этого закона ANSSI несет ответственность за: 1) определение обязательных требований безопасности для систем операторов инфраструктур; 2) проведение инспекций уровня обеспечения безопасности; 3) принятие требуемых мер в случае крупных кризисов; и 4) получение и обязательное уведомление об инцидентах, происходящих в критических системах операторов инфраструктуры. Многие из этих действий позднее появились в требованиях Директивы ЕС по вопросам безопасности сетей и инфраструктуры (EU Network and Information Security (NIS) Directive), принятой Советом Европы в мае 2016 года и вступившей в силе в августе 2016 г.[34] Франция в значительной степени уже гармонизировала свое национальное законодательство с остальными требованиями этой Директивы. Остальные действия включают в себя обеспечение того, чтобы французские банки, провайдеры телекоммуникационных услуг и ритейлеры внедряли системы обнаружения вторжений, а также сообщали о любых инцидентах в ANSSI, который имеет право проводить аудит систем и сетей любых организаций во французской юрисдикции.

ANSSI, в сотрудничестве с промышленными кругами, также выступил с дополнительными предложениями для операторов инфраструктуры с целью оказать содействие собственникам, операторам и надзорным государственным структурам в области применения норм безопасности. Кроме того, ANSSI совместно с группой партнеров запустил инициативу по аккредитации организаций – «Знак соответствия в области кибер-безопасности» (Cyber-security label) – для компаний, работающих в ИТ и секторах

обеспечения онлайн-безопасности. Цель этого процесса аккредитации – обеспечить высокие стандарты решений французских производителей в этой области как для внутреннего рынка, так и для экспорта в третьи страны.[35]

Наконец, Франция раз в два года проводит национальные учения по кризисному управлению, организуемые Генеральным секретариатом обороны и национальной безопасности (SGDSN) в рамках проекта Piranet, а также другие учения, такие как: Pirate-Air (воздушные учения), Pirate-Mer (морские учения), Pirate-Nuclear, Radiological, Biological, Chemical (NRBC) (учения в области ядерной энергетики, радиологии, биологической и химической промышленностей), а также Metro-Pirate (городская инфраструктура). В ходе каждого такого мероприятия отрабатывается национальный план действий, а сами учения проводятся в плотном режиме и с определенным уровнем секретности для обеспечения высокого уровня национальной безопасности. Планирование таких учений занимает до шести месяцев и включает в себя серию встреч между представителями SGDSN, министерств и фирм-партнеров. Во время этих встреч отрабатываются и согласовываются сценарий, цели и ход учений.[36] Франция также принимает участие в международных учениях, которые организовывает ЕС (например, Cyber Europe exercise) и НАТО (например, Locked Shields 2016). [37]

3. КИБЕРПРЕСТУПНОСТЬ И ОХРАНА ПРАВОПОРЯДКА

В 2001 г. Франция подписала, и в 2006 году ратифицировала Конвенцию по борьбе с кибер-преступностью Совета Европы (известную как Будапештская конвенция). В настоящее время страна гармонизирует свое законодательство и разрабатывает несколько законопроектов в области борьбы с кибер-преступностью. Правительство Франции поддерживает идею упрощения юридического сотрудничества между странами ЕС для облегчения обмена данными в целях борьбы с кибер-преступностью.[38]

Закон о военном планировании от 2013 г. был составлен в соответствии с требованиями «Белой книги по вопросам национальной обороны и безопасности» 2013 года, в частности, в нем содержатся призывы к организациям государственного и частного сектора соблюдать нормы кибер-безопасности, обеспечить собственную защиту (при содействии ANSSI) от потенциальных кибер-атак.[39]

В 2015 году, после нападения на редакцию еженедельника «Шарли Эбдо», в Национальной Ассамблее был утвержден «Билль о спецслужбах» (Intelligence Bill), который позволил этим организациям проводить мониторинг коммуникаций по телефону, электронной почте, а также отслеживать страницы, посещаемые в

интернете людьми, подозреваемыми в связях с террористами. Также были внесены изменения в некоторые законодательные акты, позволяющие правительству блокировать сайты, которые, по мнению правительства, «симпатизируют террористическим организациям». Также, законодательство позволяет сейчас отслеживать активность подозреваемых лиц в соцсетях.[40] Однако в ходе реализации новых норм возникли весьма серьезные проблемы с точки зрения судебного расследования и устранения контента, что привело к развитию конфликтных ситуаций в сотрудничестве с провайдерами услуг.[41]

Кроме прочего, правительство Франции также внесло изменения в другие законы, имеющие отношение к кибер-пространству.[42] Так, в январе 2016 г. Национальная Ассамблея приняла закон «Цифровая республика», тем самым законодательно утвердив меры, необходимые для реализации национальной цифровой стратегии 2011 г.[43] Закон также содержал некоторые изменения в «Закон о защите данных» (Data Protection Act) 1978 года, который подвергался изменениям уже девять раз, включая последние изменения в 2014 г.[44] В частности, решение парламента расширяло полномочия Национальной комиссии по информационным технологиям и свободам (Commission Nationale de l'Informatique et des Libertes, CNIL), предоставляя ей право налагать штрафы за нарушение приватности, в том числе если такие нарушения связаны с преступной деятельностью.[45]

В 2014 году Министерство внутренних дел создало должность "кибер-префекта", который координирует кибер-инициативы, а также реализацию плана действий МВД.

Ответственность за борьбу с кибер-преступностью несут полиция и Жандармерия Министерства внутренних дел (МВД). Жандармерия – вооруженные силы, исполняющие гражданские правоохранительные функции – с конца 1990-х годов создала многочисленные отделы по борьбе с кибер-преступностью, в т. ч.: Департамент по юридическим исследованиям и документации в области кибер-преступности (STRDJ), Институт криминалистических исследований Жандармерии (IRCGN), Центр борьбы с цифровой преступностью (C3N), Национальный центр борьбы с детской порнографией (CNAIP), а также специальные подготовительные программы при Национальном центре обучения полиции (CNFPJ).[46] Кроме того, в 2014 году МВД создало должность «кибер-префекта», в рамках которой координируется реализация инициатив МВД в области борьбы с кибер-преступностью и кибер-шпионажем, а также реализация плана Министерства в этой области. Этот план действий

ставит три стратегические цели: занятие более активной позиции в вопросах борьбы с кибер-преступностью и поддержке ее жертв, обеспечение более активного диалога со всеми заинтересованными сторонами, а также принятие необходимых национальных и международных актов и соглашений в этой области.[47]

4. ОБМЕН ИНФОРМАЦИЕЙ

Национальная кибер-стратегия 2015 г. указывает, что Франция привержена созданию национальных и международных партнерств для обмена важнейшими данными (т.е. информацией об уязвимостях или недостатках в электронных товарах и услугах) для обеспечения эффективной реализации стандартов и мер безопасности во всех критически важных секторах экономики. ANSSI несет ответственность как за координацию реагирования на кибер-инциденты, так и обмен информацией на национальном уровне. Несмотря на то, что требование применять стандарты безопасности для всех операторов критически важных элементов инфраструктуры было узаконено в 2013 г. в рамках Закона о военном планировании, это требование не вступало в силу три последующие года. Требования и Закон вступили в силу 1 июля 2016 г., что дало ANSSI и профильным организациям достаточный срок для завершения переговоров по наиболее оптимальному механизму обмена информацией и реализации стандартов кибер-безопасности, а также повышению уровня кибер-защиты. [48]

Кроме прочего, Закон о военном планировании 2013 г. требует от операторов элементов инфраструктуры информировать ANSSI об инцидентах, которые представляют опасность для функционирования соответствующих ИТ-систем. Требования касаются операторов, реализующих деятельность в различных секторах, в том числе в области здравоохранения, систем обеспечения, телекоммуникаций, транспорта и финансов. В контексте требований закона были созданы несколько рабочих групп, по одной на каждый сектор, с тем, чтобы определить и установить эффективные и применимые правила безопасности. Кроме того, закон «Цифровая республика» 2016 г. содержит три положения для расширенного обмена информацией государственного сектора с гражданами и другими частными организациями, в том числе, с результатами исследований по кибер-безопасности, не носящих секретный характер. [49]

Французский национальный центр анти-ботнет поддержки оказывает содействие частному сектору в устранении вирусного ПО и обнаружении зараженных сайтов.

Несмотря на то, что во Франции, помимо ANSSI, не создана государственная организация, ответственная за обмен информацией, в стране действуют и другие механизмы и средства такого обмена, включая некоммерческие исследовательские центры. Так, в 2014 г. был создан Французский национальный центр анти-ботнет поддержки (Antibot.fr), который вошел в некоммерческую сеть 14 стран ЕС, финансируемую Европейской комиссией в рамках Программы поддержки реализации ИКТ политики (the ICT Policy Support Program) для пилотных программ. Этот центр, созданный совместными усилиями Французского экспертного центра по борьбе с кибер-преступностью (CECyF) и организации Signal Spam, предоставляет информацию, необходимую для оперативной борьбы с бот-сетями. Он также оказывает содействие частному сектору в устранении вирусного ПО, обнаружении зараженных сайтов и аномалий в работе веб-ресурсов. [50] Наконец, во Франции существуют по крайней мере 20 секторных Команд быстрого реагирования (CERTs), которые участвуют в процессе обмена информации в секторах, в которых осуществляют свою деятельность.[51]

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

Цифровая стратегия Франции 2011 г. подчеркивает важность инвестиций в разработку инструментов обеспечения кибер-безопасности для поддержки дальнейшего экономического роста. В стратегии указывается, что правительство планирует инвестировать 150 млн. евро (примерно 170 млн. долларов США) в разработку инструментов в пяти стратегических областях: интернет вещей, суперкомпьютеры, облачные вычисления, анализ больших данных, а также безопасность информационных сетей.[52] Французское правительство в рамках этой стратегии создало «Программу национальных инвестиций», призванную оказать поддержку проектам в области облачных вычислений, что стало еще более актуальным в пост-Сноуденовские годы.[53] Пять проектов получили государственное финансирование на общую сумму в 19 млн. евро (примерно 21 млн. долларов США): CloudForce компании Orange, CloudPort компании Prologue, Magellan компании Bull, Nu@age компании Non Stop System, и UnivCloud компании INEO.

Цифровая стратегия также предусматривает оказание поддержки инкубаторам малых программ. Так, правительство Франции выделило 200 млн. евро (примерно 227 млн. долларов США) сайту-инкубатору Halle Freyssinet, на котором предполагалось разместить более тысячи стартап-проектов в 2016 г.[54]

Во Франции также расположены инновационные ИКТ-кластеры, такие как Cap Digital в регионе Иль де Франс, в рамках которого создается и распространяется цифровой контент мультимедийными способами; Images et Réseaux в Бретани и Пеи-де-ла-Луар, который специализируется на развитии коммуникационных сетей; Secure Communication Solution в Провансе, со специализацией на технологиях безопасного процессинга и коммуникаций; а также Systematic в регионе Иль де Франс, где создаются комплексные системы и программные средства оснащения устройств.[55]

В октябре 2012 г. правительство Франции опубликовало план «Проект Большой Париж: построение цифрового города». Эта программа призвана стимулировать создание в Париже и в его пригородах кластеров мирового уровня для ИТ-компаний. Это позволит собрать вместе ведущих игроков в секторе ИКТ, чтобы обеспечить дальнейший рост и стимулировать конкуренцию и инвестиции. Кроме того, бывший министр по телекоммуникациям Флёр Пельрен, провозгласила начало инициативы “La French Tech”, в рамках которой наиболее динамично развивающиеся города с высокой стартап-культурой получают статус «Метрополий французских технологий» (Métropoles French Tech). Инициатива финансируется из инвестиционного фонда в размере 200 млн. евро (примерно 223,4 млн. долларов США), целью которого является превращение страны в «цифровую республику» с участием государственных и частных партнеров.[56]

Правительство Франции также создало различные исследовательские кафедры, которые финансируются оборонными предприятиями при поддержке оборонных ведомств: Кафедра кибер-стратегии Кастекс (Castex Chair) при Институте изучения национальной безопасности (IHEDN). Этот институт обеспечивает тренинги и обучение для управленцев высшего звена из правительственных и оборонных ведомств, а также является местом для проведения дискуссий по стратегическим вопросам обороны, внешней политики, вооружений и оборонной экономики. Существуют и другие центры подобного рода, например – Кафедра кибер-безопасности в Особой военной школе (École Spéciale Militaire) в Сен-Сире, которая занимается в основном исследованиями сухопутных войск, а также Кафедры ВМС и ВВС в том же заведении, которые специализируются на исследованиях в соответствующих родах войск.[57]

Развитие сферы кибер-исследований во Франции является одной из важнейших целей правительства, которое стремится «превратить регион Ренн в крупнейший кибер-хаб во Франции и Европе».[58] «Белая книга по вопросам национальной обороны и безопасности» 2013 года призывает к более тесному сотрудничеству между органами правительства и

промышленным сектором в деле борьбы с кибер-угрозами. На основе этой задачи Министерство обороны в 2014 году создало Центр по вопросам кибер-безопасности (Pôle d'Excellence Cyber, PEC). Центр располагается в Бретани, в помещениях Генерального директората по вооружениям и информационной безопасности, который несет ответственность за обучение и повышение квалификации кибер-специалистов Министерства обороны, а также за исследования и развитие технологий в этой области. В регионе Ренн расположена крупная сеть центров, включающая центр обучения Минобороны, Генеральный директорат по вооружениям и информационной безопасности; Аналитический центр оборонных кибер-операций Минобороны (Centre d'Analyse et de Lutte Informatique Defensive, CALID, в котором базируется армейская команда быстрого реагирования MilCERT), Центр армейских коммуникаций, 807-я рота по кибер-обороне, Центр обучения коммуникациям, Особая военная школа в Сен-Сире, а также университеты и оборонные производства.[59]

В задачи Центра по вопросам кибер-безопасности (PEC) также входит разработка тренингов и симулирующих реальные условия устройств и ПО, которые могли бы использоваться Вооруженными силами и гражданскими организациями.[60] Так, в 2016 г. PEC провел соревнование Cyber West Challenge (CWC), в котором приняли участие стартапы, специализирующиеся на кибер-безопасности и обороне. Соревнованию CWC оказывают поддержку партнеры из ИКТ-сектора, в т. ч. компании, банки, воинские подразделения и Университет Южной Бретани. Победители CWC получают конкретную поддержку своим стартапам в сфере кибер-защиты – им предлагается выделенное безопасное пространство для развития в непосредственной близости к крупным подрядчикам. В рамках соревнования также планируется создать кибер-инкубатор, который создаст благоприятные условия для исследований, разработки, обучения и взаимодействия с военными

Правительство Франции стремится «превратить регион Ренн в крупнейший кибер-хаб во Франции и Европе.

властями в идеальном географическом расположении.[61] Реализуются также и другие межведомственные программы с участием университетов, французских компаний, а также правительственных органов.

Наконец, в 2013 году правительство Франции приступило к реализации нового плана развития промышленности, получившего название «Новая промышленная Франция».[62] Вторая

фаза этого плана – «Промышленность будущего» - стартовала в мае 2015 года. Ее цель - подготовка французской промышленности к цифровому будущему. План включает региональные планы для 34 промышленных районов, и в некоторые из этих региональных планов включен кибер-компонент: умные сети, цифровые больницы, обработка больших данных, облачные вычисления, электронное образование, «дополненная реальность», бесконтактные услуги, суперкомпьютеры, робототехника и кибер-безопасность. На финансирование этой инициативы правительство Франции выделило 3,7 млрд евро (примерно 4,1 млрд долларов США).[63]

6. ДИПЛОМАТИЯ И ТОРГОВЛЯ

Национальная кибер-стратегия 2015 г. поддерживает «сотрудничество стран ЕС для создания европейской стратегической цифровой автономии, как долгосрочной гарантии более безопасного кибер-пространства, в котором уважаются наши ценности».[64] Кроме того, в стратегии делается упор на стремление правительства Франции упрочить свои «активность и влияние в международном диалоге по вопросам кибер-безопасности... а также создать новые регулятивные механизмы, направленные на предотвращение возникновения конфликтов в кибер-пространстве... и консолидировать глобальную систему обязательств добросовестного поведения государств в кибер-пространстве, в соответствии с нормами международного права».[65]

В соответствии с этими целями, изложенными в национальной стратегии кибер-безопасности, Франция регулярно принимает участие в международных переговорах по вопросам кибер-безопасности, а также является членом всех ведущих международных организаций, занимающихся кибер-проблематикой, в частности – ООН, которая признала применимость международного права к кибер-пространству в 2013 г.[66] Франция считается «ведущей кибер-державой» в составе Группы правительственных экспертов ООН (UN GGE) по вопросам развития в области информации и телекоммуникаций в контексте международной безопасности, согласно отчету которой за 2013 год, «применимость международного права для кибер-пространства» является ключевым пунктом.[67] В 2015 году Группа правительственных экспертов согласовала текст нового отчета, в котором содержится проект норм ответственного поведения государств, а также список комментариев по вопросу применимости международного права в кибер-пространстве. Добровольные, не обязывающие нормы, содержащиеся в этом отчете, были полностью одобрены на заседании Генеральной Ассамблеи ООН в декабре 2015 г. и затем утверждены представителями стран Большой двадцатки.

Франция активно участвует в создании политики кибер-безопасности в рамках работы и других международных организаций, в т. ч. Организации по безопасности и сотрудничеству в Европе (ОБСЕ), где она представлена в Рабочей группе по информационной безопасности и конфиденциальности (Working Party on Information Security and Privacy, WPISP). Эта группа разрабатывает политические рекомендации по дальнейшему развитию информационного общества и повышения его устойчивости к внешним воздействиям.[68] Франция также входит в Рабочую группу по кибер-вопросам организации Friends of the Presidency Group при Совете Европы, которая была создана в 2012 г. Цель этой группы - создать площадку для горизонтальной координации действий стран ЕС в области обеспечения кибер-безопасности, а также использовать потенциальные области синергии их политики.[69] Франция также весьма активно участвовала в формировании «Стратегии кибер-безопасности Европейского Союза», которая была опубликована в феврале 2013 г. Европейской Комиссией и Высоким представителем ЕС по внешней политике и вопросам безопасности.[70]

Франция также является активным участником Вассенаарских соглашений по контролю за экспортом обычных вооружений, товаров и технологий двойного назначения 2013 г. Цель этих договоренностей – «поддержка регионального и международного мира и стабильности» посредством обеспечения прозрачности и большей ответственности в продаже и передаче конвенциональных вооружений, товаров и технологий двойного назначения. В рамках этих договоренностей Франция взяла на себя обязательства «в отношении контроля над вооружениями [в качестве] неотъемлемой части своей экспортной политики, которая подпадает под действие одной из самых строгих государственных процедур контроля».[71] В недавнем прошлом Франция также принимала участие в переговорах по созданию Трансатлантического торгово-инвестиционного партнерства (ТТИП), которое предусматривает наличие и развитие нескольких кибер-элементов. Однако французские власти пришли к заключению, что согласование документа об этом партнерстве в ближайшем будущем крайне маловероятно ввиду значительной критики этой идеи в Европе, особенно во Франции и Германии, где многие считают, что «это соглашение послужит «питательной средой для популистской риторики» и сослужит плохую службу экономике Европы».[72]

В 2014 г. МИД создал специальный пост – Посол Франции по вопросам кибер-дипломатии и цифровой экономики

Франция проводит политику достижения влияния на международной арене посредством увеличения инвестиций в неформальные международные форумы, которые расширяют сотрудничество между техническими и академическими сообществами и политиками, ответственными за принятие решений, а также путем содействия развитию экспорта ИКТ и его кибербезопасности на международном уровне.[73] В отличие от предыдущих инициатив, которые предпринимались различными министерствами, нынешние подходы характеризуются более структурным характером и межведомственным сотрудничеством и координацией.

Министерство иностранных дел и международного развития Франции ответственно за участие в международном сотрудничестве в области кибер-безопасности, а также за разработку внешней политики, ведущей к обеспечению свободного, открытого, безопасного и стабильного киберпространства. В октябре 2014 г. МИД создал специальный пост координатора в этой области – Посла Франции по вопросам кибер-дипломатии и цифровой экономики, который ответственен за все международное сотрудничество в области кибер-безопасности, в том числе включая соглашения по стандартам разумного управления, применимости международного права, защиты гражданских свобод и приватности, а также поддержки французских компаний на внешних рынках.[74]

7. ОБОРОНА И КРИЗИСНОЕ РЕАГИРОВАНИЕ

Министерство обороны Франции несет ответственность за защиту национальных систем обороны и оказание помощи любым национальным институтам.[75] «Белая книга по вопросам национальной обороны и безопасности» 2008 г. рассматривает вопросы повышения уровня кибер-безопасности как один из ведущих приоритетов национальной политики и рекомендует приступать к развитию «как оборонных, так и наступательных кибер-возможностей».[76] Однако еще до того, как меры, предусмотренные «Белой книгой» могли быть реализованы, вирус-червь Conficker заразил компьютеры многих оборонных информационных сетей. Эти события привели к неразберихе в коммуникациях и логистике взаимоотношений между различными службами, что оказало негативное действие на работу Вооруженных сил. Военная авиация пострадала незначительно, т.к. она обладает своими собственными средствами коммуникации, а сети с секретной информацией не пострадали вовсе.[77]

С того времени Министерство обороны активно включилось в процесс повышения уровня профессионализма, стратегической переориентации, и, в частности, активного противодействия кибер-угрозам национальной обороне и военным информационным сетям.

В 2009 г. правительство Франции создало Национальное агентство безопасности информационных систем (ANSSI) в качестве нового этапа процесса, в котором принимают участие Вооруженные силы и другие структуры, обеспечивающие безопасность в рамках работы полиции и армии. В 2011 г., в рамках национальной стратегии кибер-безопасности, «Оборона и безопасность информационных сетей: стратегия Франции», правительство объявило о намерении стать «супердержавой в вопросах кибер-обороны» и расширило полномочия ANSSI.[78] В том же году Министерство обороны, в своей Единой кибер-доктрине, объявило о создании поста Командующего по вопросам кибер-обороны (OG Cyber), а также подчиненных ему подразделений, таких как Оперативное командование кибер-обороны, расположенное в Совместном центре оперативного планирования, командования и контроля (Centre de Planification et de Conduite des Opérations, CPCO).[79] Командующий по вопросам кибер-обороны несет ответственность за безопасность информационных сетей Министерства в случае возникновения кризисных ситуаций, а также, в случае необходимости, тесно сотрудничает с ANSSI в деле защиты всех информационных сетей страны.[80]

«Белая книга по вопросам национальной обороны и безопасности» 2013 г. заменила «Белую книгу» 2008 г., еще более расширив и упрочив роль Министерства обороны в вопросах самого широкого спектра обеспечения кибер-обороны страны.[81] В этом документе правительство признает, что «кибер-пространство стало зоной конфронтации», и отмечает, что кибер-атаки «могут с легкостью парализовать целые области жизнедеятельности в стране, стать причиной технологических или экологических катастроф, и привести к многочисленным жертвам. Таким образом, такие атаки могут вполне считаться военными действиями».[82] Далее в этом же документе Министерство обороны заявляет о необходимости развития «средств выявления и противодействия кибер-атакам», считая, что такие средства являются «важнейшим фактором для реализации возможного и адекватного реагирования на кибер-атаки».[83] В документе также подтверждается, что «Министерство обороны и в дальнейшем будет продолжать свою деятельность даже в случаях (и в первую очередь именно в таких случаях), когда деятельность многих других организаций будет затруднена или невозможна в результате кибер-атак».[84]

Для реализации амбициозных задач, изложенных в «Белой книге» 2013 г., Министерство обороны объявило в 2014 г. о начале реализации Пакта кибер-обороны (Pacte Défense Cyber 2014-2016) стоимостью в 1 млрд. евро (примерно 1,1 млрд долларов США). В документе содержатся шесть

основных задач: 1) повышение уровня безопасности информационных систем Министерства и его доверенных партнеров; 2) подготовка к будущим угрозам посредством интенсификации исследовательской работы в технической, академической и операционной областях при поддержке промышленного сектора; 3) повышение уровня человеческих ресурсов в области кибер-обороны; 4) создание Центра в области кибер-обороны в Бретани для нужд Министерства и сообщества специалистов в этой области; 5) тесная работа с сетью зарубежных партнеров в Европе и регионах стратегических интересов Франции; и 6) стимулирование создания и развития сообщества специалистов в вопросах кибер-обороны на основе возникновения круга партнеров и создания резервных информационных сетей.[85] В документе перечисляются 50 мер, составляющих национальную доктрину кибер-обороны и ведущих к достижению амбициозных поставленных целей.

Эквивалент французского "кибер командования" возник при Командующем по вопросам кибер-обороны вместе с соответствующим персоналом, миссиями и возможностями

Среди этих мер – упрочение и расширение полномочий организаций, созданных в 2011 г., расширение потенциала OG Cyber, а также работа по дальнейшей операционализации подразделений, призванных осуществлять кибер-оборону и, в меньшей степени – наступление.[86] Изменения включали развитие более тесного сотрудничества с ANSSI для подготовки планов экстренных действий, в том числе включая размещение Аналитического центра оборонных кибер-операций Минобороны (Centre d'Analyse et de Lutte Informatique Defensive, CALID, в котором также располагается армейская команда быстрого реагирования MilCERT), в одном здании.[87] CALID является «центральным хранилищем экспертных данных Министерства обороны и служит также центром готовности и реагирования в случае кибер-атак Министерства; он осуществляет надзор и круглосуточное наблюдение, отслеживая кибер-атаки против армейских подразделений и сетей.[88] Кроме того, Пакт кибер-обороны требует создания национального оперативного резерва кибер-обороны (Réserve de Cyber Défense, RCD), в чьи задачи будет входить содействие Министерству обороны и государственным

организациям в случаях возникновения серьезных кризисов. Резервные подразделения будут создаваться в тесном сотрудничестве с ANSSI и Национальной Жандармерией.[89]

Все вместе эти мероприятия привели к созданию своеобразного «кибер-командования» с необходимым персоналом, задачами и потенциалом под руководством OG Cyber.[90] Если быть более точным, этот уполномоченный офицер является верхушкой оперативной цепочки командования в области кибер-безопасности в рамках системы командования Вооруженных сил Франции. OG Cyber «играет главную роль в Центре оперативного планирования, где он несет ответственность за планирование, координацию и проведение операций в области кибер-обороны информационных сетей Министерства обороны и Вооруженных сил, и кибер-операций в поддержку военных операций». Он также «несет ответственность за координацию и развитие системы кибер-обороны в рамках всего Министерства, а также трех его служб».[91] Таким образом, он является командующим кибер-подразделениями, а также руководит планированием и подготовительной работой в кибер-секции французского генштаба. Ключевой штабной офицер – Командующий компьютерными военными действиями (Officier de Lutte Informatique Defensive, OLID), отвечает за развертывание кибер-сил в рамках всех Вооруженных сил, а команда кибер-управления реализует решения OG Cyber.[92]

Статья на кибер-операции в военном бюджете была увеличена параллельно с ростом задач и подразделений. В 2014 г. Министр обороны объявил о выделении более 1 млрд евро (1,1 млрд. долларов США) на реализацию пятидесяти мер, перечисленных в Пакте кибер-обороны 2014-2016.[93] Так, в частности, выделялись средства на удвоение штата Центра по кибер-безопасности в Бретани – с 250 до 450 сотрудников. вообще же, правительство Франции соблюдает свои обязательства в рамках НАТО, обеспечивая выделение 2% и более (в частности - 2,1%) ВВП на оборонные мероприятия, причем доля средств, выделяемых на обеспечение кибер-безопасности, растет в отношении к другим расходам.[94]

Французские Вооруженные силы являются активным участником национальных и международных кибер-учений – как указывается в соответствующей главе этого обзора – а в особенности тех учений, которые проводятся в рамках НАТО, таких как «Кибер-коалиция» (Cyber Coalition). В

Пакте кибер-обороны Министерство обозначило цель «систематически включать элементы кибер-обороны в процесс армейских учений всех уровней».”[95] Учения призваны служить средством обеспечения способности Вооруженных сил действовать на уровне каждого звена в случае кибер-атак, вредоносных действий или других угроз, включая «возможность включения кибер-пространства в сферу своих действий».[96] В 2015 году Франция провела свой первый Международный форум по вопросам кибер-обороны с участием 26 иностранных делегаций, на котором рассматривались различные международные кибер-вопросы.[97]

Наконец, Министерство обороны является активным игроком в области обеспечения кибер-безопасности во время национальных кризисов. Так, во время нападения на еженедельник Шарли Эбдо и последовавших кибер-атак против гражданских и военных объектов, Генштаб Франции впервые в истории страны активировал кибер-подразделения.[98] После теракта в Ницце на День взятия Бастилии в 2016 году, Минобороны призвало как минимум 12000 резервистов, многие из которых состояли в кибер-резерве.[99]

ЗАКЛЮЧЕНИЕ: ИНДЕКС КИБЕРГОТОВНОСТИ CRI 2.0

По оценке авторов CRI 2.0, Франция находятся 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 киберготовности страны на момент написания отчета. Франция 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. Hugh Schofield, “Minitel: The rise and fall of the France-wide web,” BBC News, June 28, 2012, http://www.bbc.com/news/magazine-18610692.

2. James Foreman-Peck, “European Industrial Policies in the Post-war Boom: ‘Planning the Economic Miracle’,” in Industrial Policy in Europe After 1945, (Palgrave Macmillan UK, 2014): 14, http://www.palgraveconnect.com/pc/doifinder/view/10.1057/9781137329905.0008.

3. World Bank, “Internet users (per 100 people),” 2014, http://data.worldbank.org/indicator/IT.NET.USER.P2.

4. Premier Ministre, “France Numérique 2012-2020: Bilan et Perspectives,” November 2011, http://www.entreprises.gouv.fr/files/files/directions_services/secteurs-professionnels/etudes/2011_plan_france_numerique2020.pdf.

5. Cécile Barbière, “France launches EU’s first digital infrastructure ‘project bond,’” EuroActiv, October 15, 2015, http://www.euractiv.com/section/regional-policy/news/france-launches-eu-s-first-digital-infrastructure-project-bond/

6. Pascal Brangetto, “National Cyber Security Organisation: France,” NATO Cooperative Cyber Defense Center of Excellence (2015): 5.

7. Embassy of France in London, “France aims to put tech at the heart of its economy by 2020,” France in the United Kingdom, http://www.ambafrance-uk.org/France-aims-to-put-tech-at-heart.

8. OECD, “OECD Digital Economy Outlook 2015,” (OECD Publishing: Paris): 21, http://www.oecd.org/internet/oecd-digital-economy-outlook-2015-9789264232440-en.htm.

9. Embassy of France in London, “France aims to put tech at the heart of its economy by 2020.”

10. BPI France, “Le Fonds Amibition Numérique,” December 2, 2011, http://www.bpifrance.fr/Bpifrance/Nos-metiers/Fonds-propres/Fonds-directs-Bpifrance/Capital-Innovation/Le-Fonds-Ambition-Numerique.

11. French Senate, “Rapport Bockel,” July 18, 2012, http://www.senat.fr/notice-rapport/2011/r11-681-notice.html.

12. Premier Ministre, “French National Digital Security Strategy,” (2015), http://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf.

13. ANSSI, “Cybersecurity in France,” http://www.ssi.gouv.fr/en/cybersecurity-in-france/.

14. "2015 Paris Terror Attacks Fast Facts," CNN, April 13, 2016, http://www.cnn.com/2015/12/08/europe/2015-paris-terror-attacks-fast-facts/

15. Matthew Dalton and Sam Schechner, "France Tried to Ramp Up Defenses Ahead of Paris Attacks," The Wall Street Journal, November 14, 2015, http://www.wsj.com/articles/paris-attacks-underscore-security-challenge-1447462066.

16. "France asks US Internet giants to 'help fight terror,'" Al Jazeera, February 21, 2015, http://www.aljazeera.com/news/2015/02/france-asks-internet-giants-fight-terror-150221063706705.html.

17. "France Launches a Terrorism App," Security Magazine, June 9, 2016, http://www.securitymagazine.com/articles/87182-france-launches-a-terrorism-app.

18. Ministry of Defense, "French White Paper on Defence and National Security," (2013): 43, http://www.ladocumentationfrancaise.fr/rapports-publics/134000257-livre-blanc-sur-la-defense-et-la-securite-nationale-2013?xtor=EPR-526.

19. Ministry of Defense, "The French White Paper on Defence and National Security," (2008): 12.

20. ANSSI, "Cybersecurity in France."

21. Pascal Brangetto, "National Cyber Security Organisation: France," NATO Cooperative Cyber Defense Center of Excellence (2015): 9

22. NATO Parliamentary Assembly: Science and Technology Committee, "Cyber Space and Euro-Atlantic Security," Special Report, (November 2014): 9.

23. Premier Ministre, "Information Systems Defence and Security: France's Strategy," (2011), http://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf.

24. Ministry of Defense, "French White Paper on Defence and National Security," (2013).

25. Premier Ministre, "French National Digital Security Strategy," (2015).

26. World Bank, "Internet users (per 100 people)," http://data.worldbank.org/indicator/IT.NET.USER.P2.

27. Tom Reeve, "French government launches national cyber security strategy," SC Magazine, October 19, 2015, http://www.scmagazineuk.com/french-government-launches-national-cyber-security-strategy/article/447973/.

28. Premier Ministre, "French National Digital Security Strategy," (2015): 20.

29. ANSSI, "CERT-FR – Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques," http://www.cert.ssi.gouv.fr/.

30. ANSSI, "Plan Piranet," http://www.ssi.gouv.fr/agence/cybersecurite/plans-gouvernementaux/.

31. Ministry of Defense, "French White Paper on Defence and National Security," (2013).

32. Melissa Hathaway's interview with Valérie Derouet-Mazoyer, Coordinator of the French Nuclear Industry Strategic Committee (CSFN), September 16, 2016.

33. Legifrance, "LOI n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale," https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825.

34. European Council, "EU-wide cybersecurity rules adopted by the Council," May 17, 2016, http://www.consilium.europa.eu/en/press/press-releases/2016/05/17-wide-cybersecurity-rule-adopted/.

35. "Cyber-security: France Leads the Way in Europe," Media Econocom Blog, May 7, 2015, http://blog.econocom.com/en/blog/cyber-security-france-leads-the-way-in-europe/.

36. ANSSI, "French Cybersecurity Exercises," June 27, 2012, https://www.enisa.europa.eu/events/cyber-exercise-conference/presentations/9.%20Conf%20Paris%20-June%202012-%20-%20A.%20OGEE%20-ANSSI%20France.pdf, and ANSSI, "Cyber-attaques: l'exercice PIRANET 2012 met l'État à l'épreuve d'une crise informatique majeure," http://www.ssi.gouv.fr/publication/cyber-attaques-lexercice-piranet-2012-met-l-etat-a-lepreuve-dune-crise-informatique-majeure/.

37. Thomas Renard, "The Rise of Cyber Diplomacy: the EU, its Strategic Partners, and Cyber- Security," European Strategic Partnerships Observatory 7 (June 2014): 14, http://www.egmontinstitute.be/wp-content/uploads/2014/06/ESPO-WP7.pdf.

38. Government of France, "French National Digital Security Strategy," (2015): 23.

39. Legifrance, "LOI n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale," https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825.

40. Alessandria Masi, "France's online war on terror sympathizers and extremists has a new cyber security cell," IBT, http://www.ibtimes.com/frances-online-war-terror-sympathizers-extremists-has-new-cyber-security-cell-1786662.

41. Melissa Hathaway's interview with Frédérick Douzet (Ph.D.), Chairwoman of the Castex Chair of Cyber Strategy and Professor at the French Institute of Geopolitics, Paris 8 University, September 8, 2016.

42. Premier Ministre, "French National Digital Security Strategy," (2015): 15.

43. Government of France, "Explanatory Memorandum," January 2016, http://www.republique-numerique.fr/pages/digital-republic-bill-rationale.

44. Commission Nationale de l'Informatique et des Liberties, "Loi Informatique et Libertes, Act No. 78-17 January 1978 on Information Technology, Data Files and Civil Liberties," (January 1978), https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf.

45. Nadège Martin and Geoffroy Coulouvrat, "French National Assembly adopts "Digital Republic" bill," Norton Rose Fulbright, March 10, 2016, http://www.dataprotectionreport.com/2016/03/french-national-assembly-adopts-digital-republic-bill/.

46. Gendarmerie Nationale, "Cybercriminalité," http://www.gendarmerie.interieur.gouv.fr/Notre-Institution/Nos-missions/Police-judiciaire/Cybercriminalite.

47. Government of France, "Cybersecurity: the Government's Strategy," January 28, 2016, http://www.gouvernement.fr/en/cybersecurity-the-government-s-strategy.

48. Reynald Fléchaux, "Cybersécurité : les grandes entreprises trouvent un modus vivendi avec l'Assi," Silicon, January 26, 2016, http://www.silicon.fr/cybersecurite-grandes-entreprises-trouvent-modus-vivendi-anssi-136930.html.

49. Samuel Greengard, "France Embraces Digital Transformation," Communications of the ACM, June 3, 2016, http://cacm.acm.org/news/203101-france-embraces-digital-transformation/fulltext.

50. Antibot, "Lancement d'Antibot.fr," December 10, 2014, http://www.antibot.fr/blog/lancement-d-antibot.fr.

51. ANSSI, "Les CSIRT Français," http://www.cert.ssi.gouv.fr/cert-fr/cert.html.

52. OECD, "OECD Digital Economy Outlook 2015," (OECD Publishing: Paris): 24.

53. Melissa Hathaway's interview with Frédérick Douzet (Ph.D.), September 8, 2016.

54. Ibid.

55. Embassy of France in London, "France aims to put tech at the heart of its economy by 2020," France in the United Kingdom, http://www.ambafrance-uk.org/France-aims-to-put-tech-at-heart.

56. Ibid.

57. Melissa Hathaway's interview with Frédérick Douzet (Ph.D.), September 8, 2016.

58. Philippe Vitel and Henrik Bliddal, "French Cyber Security and Defence: An Overview," Information & Security: An International Journal, vol. 32 (2015): 9, http://connections-qj.org/system/files/3209_france.pdf.

59. Ibid.

60. Ministry of Defense, "Cyber Defence Pact: 50 Measures to Change Scale," (2014): 16.

61. "Cyber West Challenge," http://www.cyberwestchallenge.bzh/en/.

62. Embassy of France in London, "The Industry of the Future," September 17, 2015, http://www.ambafrance-uk.org/The-Industry-of-the-Future, and http://tradebridgeconsultants.com/news/government/president-francois-hollande-launches-new-industrial-france/

63. Trade Bridge Consultants, "President François Hollande launches 'New Industrial France'," http://tradebridgeconsultants.com/news/government/president-francois-hollande-launches-new-industrial-france/.

64. Premier Ministre, "French National Digital Security Strategy," (2015): 9.

65. Legifrance, "LOI n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale," https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825 and Alessandria Masi, "France's online war on terror sympathizers and extremists has a new cyber security cell," http://www.ibtimes.com/frances-online-war-terror-sympathizers-extremists-has-new-cyber-security-cell-1786662.

66. OECD, "OECD Digital Economy Outlook 2015," http://www.oecd.org/internet/oecd-digital-economy-outlook-2015-9789264232440-en.htm.

67. CCDCOE, "2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law," August 31, 2015, https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html.

68. Thomas Renard, "The Rise of Cyber-Diplomacy: the EU, its Strategic Partners and Cyber-Security," European Strategic Partnership Observatory, (June 2014):12, http://www.egmontinstitute.be/wp-content/uploads/2014/06/ESPO-WP7.pdf.

69. Ibid, 13.

70. Ministry of Foreign Affairs, "France and Cyber Security," December 2014, http://www.diplomatie.gouv.fr/en/french-foreign-policy/defence-security/cyber-security/.

71. "French Policy on Export Controls for Conventional Arms and Dual-Use Goods and Technologies," http://www.wassenaar.org/wp-content/uploads/2015/12/fr1_en.pdf.

72. AFP, "EU-US trade deal 'impossible' in 2016: French minister Matthias Fekl," The Economic Times, July 5, 2016, http://economictimes.indiatimes.com/news/international/business/eu-us-trade-deal-impossible-in-2016-french-minister-matthias-fekl/articleshow/53065263.cms.

73. Premier Ministre, "French National Digital Security Strategy," (2015): 40.

74. Ministry of Foreign Affairs, "France and Cyber Security," December 2014, http://www.diplomatie.gouv.fr/en/french-foreign-policy/defence-security/cyber-security/.

75. Pascal Brangetto, "National Cyber Security Organisation: France," NATO Cooperative Cyber Defense Center of Excellence (2015): 11.

76. Ministry of Defense, "The French White Paper on Defence and National Security," (2008): 9.

77. Kim Willsher, "French Fighter Plans Grounded by Computer Virus," The Telegraph, February 7, 2009, http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html.

78. Premier Ministre, "Information Systems Defence and Security: France's Strategy," ANSSI, (2011), http://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf.

79. Ministry of Defense, "Cyber Defence Pact: 50 Measures to Change Scale," (2014): 5.

80. Ministry of Foreign Affairs, "France and Cyber Security."

81. "Europe Proposes New Laws and Regulations on Cybersecurity," Jones Day, January 2014, http://www.jonesday.com/europe-proposes-new-laws-and-regulations-on-cyber-security-01-02-2014/.

82. Ministry of Defense, "French White Paper on Defence and National Security," (2013): 4, 43.

83. Embassy of France in London, "France aims to put tech at the heart of its economy by 2020," http://www.ambafrance-uk.org/France-aims-to-put-tech-at-heart.

84. Ministry of Defense, "Cyber Defence Pact: 50 Measures to Change Scale," (2014): 5.

85. Ministry of Defense, "Présentation du Pacte Défense Cyber," November 2, 2014, http://www.defense.gouv.fr/actualites/articles/presentation-du-pacte-defense-cyber.

86. Ministry of Defense, "Cyber Defence Pact: 50 Measures to Change Scale," (2014): 6-9.

87. NATO Parliamentary Assembly: Science and Technology Committee "Cyber Space and Euro-Atlantic Security," Special Report (November 2014): 9.

88. Michel Baud, "American Military Cyberdefense, an Example for France?," Chaire de CyberDéfense et Cybersecurité, Saint-Cyr Publication Series, vol. 111, n. 8, (July 2013): 1-3.

89. Philippe Vitel and Henrik Bliddal, "French Cyber Security and Defence: An Overview," (2015): 9.

90. CyberDef-CyberSec, "4th Cyber Def – Cyber Sec Conference 2016," June 14, 2016, Paris.

91. Philippe Vitel and Henrik Bliddal, "French Cyber Security and Defence: An Overview," (2015): 8.

92. Michel Baud, "American Military Cyberdefense, an Example for France?", 3.

93. Ministry of Defense, "Cyberdéfense," Direction Général des Relations Internationales et de la Stratégie, June 22, 2016, http://www.defense.gouv.fr/dgris/enjeux-transverses/cyberdefense/cyberdefense.

94. Pascal Brangetto, "National Cyber Security Organisation: France," (2015): 12.

95. Ministry of Defense, "Cyber Defence Pact: 50 Measures to Change Scale," (2014): 9.

96. Embassy of France in London, "France aims to put tech at the heart of its economy by 2020."

97. Melissa Hathaway's interview with Frédérick Douzet (Ph.D.), September 8, 2016.

98. Nathalie Guibert, "Cyberattaques: l'armée a activé pour la première fois une cellule de crise," Le Monde, January 1, 2015, http://www.lemonde.fr/pixels/article/2015/01/17/cyberattaques-l-armee-a-active-pour-la-premiere-fois-une-cellule-de-crise_4558160_4408996.html?xtmc=cyber&xtcr=1.

99. "Nice attack: France calls up to 12,000 reservists," BBCNews, July 17, 2016, http://www.bbc.com/news/world-europe-36817435.

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