Организация Объединенных Наций A/74/120

Генеральная Ассамблея

Distr.: General
24 June 2019
Russian
Original: English/French/Spanish

Семьдесят четвертая сессия
Пункт 95 первоначального перечня*

Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Доклад Генерального секретаря

Содержание

* A/74/50.

19-10580 (R) 250719 300719

I. Введение

1. На своей семьдесят третьей сессии Генеральная Ассамблея приняла две резолюции по пункту 96 повестки дня о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности.

2. 5 декабря 2018 года Генеральная Ассамблея приняла резолюцию 73/27 о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности, а 22 декабря — резолюцию 73/266 о поощрении ответственного поведения государств в киберпространстве в контексте международной безопасности.

3. В пункте 4 резолюции 73/27 Генеральная Ассамблея просила все государства-члены продолжать, принимая во внимание оценки и рекомендации, содержащиеся в докладах Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, информировать Генерального секретаря о своей точке зрения и об оценках по следующим вопросам:

a) общая оценка проблем информационной безопасности;

b) усилия, предпринимаемые на национальном уровне для укрепления информационной безопасности и содействия международному сотрудничеству в этой области;

c) содержание концепций, упомянутых в пункте 3 этой резолюции;

d) возможные меры, которые могли бы быть приняты международным сообществом для укрепления информационной безопасности на глобальном уровне.

4. В пункте 2 резолюции 73/266 Генеральная Ассамблея просила все государства-члены продолжать, принимая во внимание оценки и рекомендации, содержащиеся в докладах Группы правительственных экспертов, информировать Генерального секретаря о своей точке зрения и об оценках по следующим вопросам:

a) усилия, предпринимаемые на национальном уровне для укрепления информационной безопасности и содействия международному сотрудничеству в этой области;

b) содержание концепций, упомянутых в докладах Группы правительственных экспертов.

5. В соответствии с этой просьбой 6 февраля 2019 года всем государствам-членам была направлена вербальная нота, в которой им было предложено представить информацию по этому вопросу. Ответы, полученные на момент составления настоящего доклада, содержатся в разделе II. Дополнительные ответы, полученные после 15 мая 2019 года, будут размещены на веб-сайте Управления по вопросам разоружения (www.un.org/disarmament/ict-security) на том языке, на котором они были представлены.

II. Ответы, полученные от правительств

Аргентина

[Подлинный текст на испанском языке]
[15 мая 2019 года]

Общая оценка проблем информационной безопасности

Информационно-коммуникационные технологии (ИКТ) открывают беспрецедентные возможности для экономического, социального, культурного, научного и политического прогресса, и развитие этих технологий неразрывно связано с повышением уровня развития и благосостояния. Виртуальное пространство стало неотъемлемым элементом деятельности людей и организаций, и все больше жизненно важных услуг оказывается с помощью компьютерных сетей.

Обеспечивая беспрецедентный уровень взаимодействия и прогресса, киберпространство вместе с тем становится объектом огромного количества угроз различного характера и действий злоумышленников, которые ставят под угрозу безопасность людей, предприятий, учреждений и государств и представляют собой опасность для международного мира и безопасности.

Экономическое развитие, предоставление основных услуг, благосостояние граждан и надлежащее функционирование государственных учреждений в значительной степени зависят от кибербезопасности.

Что касается новых рисков, то их рост связан с широким распространением относительно недорогих интеллектуальных устройств, предоставляющих доступ к Интернету без малейшей попытки обеспечить даже минимальный уровень безопасности, что увеличивает вероятность совершения кибератак.

Для того чтобы противостоять росту этих угроз, необходимо проводить соответствующую государственную политику и реализовывать такие стратегии корпоративной ответственности, которые позволили бы решить эту проблему.

Кроме того, проекты, в рамках которых государства задействуют какой-либо механизм, позволяющий им расшифровывать информацию с устройств/приложений, и/или инструмент обхода системы защиты, сопряжены с дополнительными рисками.

Усилия, предпринимаемые на национальном уровне в целях укрепления информационной безопасности

В 2017 году правительство Аргентины указом 577/2017 учредило Комитет по кибербезопасности под председательством секретариата правительства по модернизации канцелярии кабинета министров и при участии секретариата по стратегическим вопросам канцелярии кабинета министров, Министерства обороны, Министерства безопасности, Министерства иностранных дел и по делам религий и Министерства юстиции и по правам человека. В число функций Комитета входит разработка национальной стратегии кибербезопасности и плана действий по ее реализации.

С учреждением Комитета по кибербезопасности были созданы условия для обмена информацией об инцидентах, что позволило улучшить координацию мер реагирования; это доказало свою эффективность в ходе работы Группы 20 в Аргентине в 2018 году.

В Аргентине действует национальная программа по критически важной информационной инфраструктуре и кибербезопасности, разработанная в соответствии с резолюцией 580/2011 канцелярии кабинета министров и направленная, в частности, на определение и защиту стратегической и критически важной инфраструктуры государственного и частного секторов и межюрисдикционных организаций, а также на управление всей информацией о сообщениях об инцидентах в области безопасности и на изыскание возможных решений организованным и унифицированным образом.

В этом контексте для государственных органов был разработан протокол на случай возникновения повышенного риска информационной безопасности, предусматривающий связь с частным сектором.

В настоящее время ведется работа по разработке стандарта, согласно которому будут определяться критически важные информационные инфраструктуры, критерии установления их критичности и их категоризация в различных секторах.

В рамках национальной программы по критически важной информационной инфраструктуре и кибербезопасности распоряжением № 2/2013 была создана национальная группа по реагированию на чрезвычайные ситуации в компьютерной сфере.

Что касается законодательства, то в 2008 году Законом № 26.388 компьютерные преступления были включены в Уголовный кодекс. В 2013 году Национальный конгресс утвердил Закон № 26.904, который предусматривает уголовную ответственность за обхаживание детей в Интернете с целью склонить их к действиям сексуального характера («груминг») и ужесточает наказание за преступления, связанные с детской порнографией в Интернете. В 2017 году Конгресс принял Закон 27.411 о присоединении к Конвенции о киберпреступности. В январе 2019 года Конгресс утвердил Закон № 27.482 о внесении изменений в Федеральный уголовно-процессуальный кодекс, который предусматривает меры получения цифровых доказательств (изъятие цифровых сообщений, регистрация и хранение данных и компьютерных систем).

В настоящее время ведется работа над законопроектом о внесении изменений в Уголовный кодекс, предусматривающим криминализацию ряда компьютерных преступлений и, в частности, посягательств на важнейшие объекты инфраструктуры.

В целях расширения возможностей борьбы с киберпреступностью министерство юстиции и по правам человека в сотрудничестве с такими международными организациями, как Организация американских государств (ОАГ) и Совет Европы, провело для работников системы уголовного правосудия целый ряд семинаров по вопросам киберпреступности, обработки цифровых улик и современных форм расследования. Эти семинары проводились в различных регионах страны и были ориентированы на судей, следователей и сотрудников сил безопасности на федеральном и провинциальном уровнях. С 2016 года по настоящее время в этих учебных программах приняли участие почти 500 судей и следователей по всей стране.

Одной из целей плана действий Аргентины в области цифровых технологий, утвержденного Указом 996/2018, является наращивание потенциала в области кибербезопасности в целях укрепления доверия к цифровой среде. В этой связи в координации с программой «Цифровая точка» были разработаны учебные программы для инструкторов, направленные на укрепление потенциала для повышения осведомленности населения в целом и групп риска в частности о рисках, связанных с использованием социальных сетей и Интернета. В ходе этих

программ рассматривались такие темы, как травля в Интернете («кибербуллинг»), «груминг», сетевое мошенничество («фишинг»), кибербезопасность и стратегии оказания помощи жертвам, предупреждения и выявления компьютерных преступлений, причем особое внимание уделялось в этой связи молодежи, подросткам и пожилым людям.

Что касается защиты персональных данных, то Аргентина одной из первых в регионе создала нормативную базу для защиты персональных данных, приняв Закон № 25.326. Аргентина является участницей Конвенции Совета Европы о защите частных лиц в отношении автоматизированной обработки данных личного характера.

С 1 июня 2019 года в Аргентинской Республике вступит в силу Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера и Дополнительный протокол к ней.

Усилия, предпринимаемые для содействия международному сотрудничеству в области информационной безопасности

Аргентина выступает за разработку двусторонних, региональных и многосторонних соглашений, способствующих созданию мирного и безопасного киберпространства, и стремится обеспечить свое присутствие во всех международных организациях, занимающихся вопросами кибербезопасности, и активно участвовать во всех международных научно-технических мероприятиях, на которых ведется работа по этой теме.

В этой связи она активно участвует в деятельности Комитета по Конвенции о киберпреступности и поддерживает государства, которые еще не стали ее участниками, но желают ими стать. К числу конкретных преимуществ, которыми пользуются участники этого договора, относится участие в круглосуточной сети, обеспечивающей канал сотрудничества и содействующей в проведении уголовных расследований между различными государствами-участниками.

Вместе с тем, принимая во внимание транснациональный характер киберпреступности и необходимость наличия механизмов, позволяющих принимать глобальные ответные меры, Аргентина поддерживает как процессы, осуществляемые в рамках Конвенции о киберпреступности, так и обсуждения, нацеленные на проведение в рамках Организации Объединенных Наций переговоров об универсальной правовой базе по данному вопросу (Венский процесс).

Аргентина принимала участие в работе Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности состава 2013 и 2014 годов и стремится внести свой вклад в обсуждения по этому вопросу в Генеральной Ассамблее.

Осознавая важность наращивания потенциала, Аргентина является членом Глобального форума по обмену опытом в области компьютерных технологий и вместе с ОАГ, Испанией, Мексикой, Чили и Эстонией участвует в реализации Инициативы по кибербезопасности в государствах — членах ОАГ.

В ноябре 2018 года Аргентина присоединилась к Парижскому призыву к доверию и безопасности в киберпространстве.

На региональном уровне Аргентина участвует в заседаниях Рабочей группы по мерам укрепления сотрудничества и доверия в киберпространстве, созданной Межамериканским комитетом ОАГ по борьбе с терроризмом, и внесла вклад в деятельность Наблюдательного совета по кибербезопасности в Латинской Америке и Карибском бассейне, предоставив информацию для второго издания исследования «Кибербезопасность: подготовлены ли мы в

Латинской Америке и Карибском бассейне?», проведенного ОАГ и Межамериканским банком развития.

29–30 мая 2018 года в Аргентине проходил II Международный форум по гендерным вопросам и кибербезопасности, организованный совместно с ОАГ.

В рамках Южноамериканского общего рынка (МЕРКОСУР) Аргентина содействует разработке плана действий МЕРКОСУР в области цифровых технологий, в который включены и вопросы кибербезопасности.

На двустороннем уровне в 2017 году Аргентина подписала с Испанией межучрежденческий меморандум о взаимопонимании по вопросам кибербезопасности. В том же году Аргентина и Соединенные Штаты договорились сформировать двустороннюю межправительственную рабочую группу по вопросам политики в киберпространстве, которая займется, в частности, вопросами кибербезопасности, а в 2018 году Аргентина подписала с Чили соглашение о сотрудничестве в области кибербезопасности, киберпреступности и киберзащиты. Аргентина считает важным поддерживать открытые каналы диалога по вопросам кибербезопасности со всеми странами и регионами.

Замечания по содержанию докладов Группы правительственных экспертов, резолюции 73/27 Генеральной Ассамблеи и мерам, которые международное сообщество могло бы принять для укрепления информационной безопасности на глобальном уровне

Аргентина поддерживает и разделяет содержание концепций, упомянутых в докладах Группы правительственных экспертов.

На государства возложена задача поддержания безопасного и мирного киберпространства, для выполнения которой крайне важно обеспечить ответственное поведение путем применения норм действующего международного права, разработки новых добровольных норм, расширения международного сотрудничества и принятия мер укрепления доверия в соответствии с резолюциями 69/28, 70/237, 71/28, 73/187 и 73/266 Генеральной Ассамблеи, посвященными этому вопросу.

Для того чтобы государства, нуждающиеся в совершенствовании своих систем предупреждения, обнаружения, оповещения и реагирования на угрозы в киберпространстве, могли укрепить свой потенциал, крайне необходимо обеспечить двустороннее, региональное и многостороннее сотрудничество.

Эффективная борьба с киберпреступностью является одним из важнейших элементов обеспечения безопасности и мира в киберпространстве и, следовательно, вопросом первостепенной важности для сотрудничества между государствами.

Что касается резолюции 73/27 Генеральной Ассамблеи, в частности свода международных правил, норм и принципов ответственного поведения государств, о которых говорится в пункте 1 резолюции, то Аргентина разделяет их актуальность. Вместе с тем следует отметить, что, учитывая характер угроз в киберпространстве и скорость их развития, необходимо, чтобы государства прилагали все возможные усилия к тому, чтобы не допустить использования их территории негосударственными субъектами для совершения международно-противоправных действий с использованием ИКТ. Однако нельзя утверждать, что они могут это гарантировать.

Кроме того, учитывая глобальный и транснациональный масштаб угроз в киберпространстве, международному сообществу следует уделять больше внимания наращиванию потенциала, с тем чтобы все государства, в частности

развивающиеся страны, укрепили свои системы предупреждения, обнаружения, оповещения и реагирования на угрозы в киберпространстве.

Аргентина полагает, что необходимо продолжать работу в рамках таких процессов Организации Объединенных Наций, как Группа правительственных экспертов и Рабочая группа открытого состава по достижениям в области информатизации и телекоммуникаций в контексте международной безопасности, учрежденная резолюцией 73/27 Генеральной Ассамблеи. Крайне важно достичь консенсуса в отношении применения международного права в киберпространстве, для чего необходимо обеспечить диалог и транспарентность в отношении программы действий каждого государства. Кроме того, решающее значение имеет разработка таких механизмов и инструментов, которые могут быстро адаптироваться к изменениям и новым вызовам, постоянно возникающим в связи с ускоренным развитием технологий.

Колумбия

[Подлинный текст на испанском языке]
[15 мая 2019 года]

Общие соображения

Правительство Колумбии согласно с тем, что необходимо укреплять координацию и сотрудничество между государствами в целях изучения угроз и возможных совместных мер по их устранению, применения норм международного права при использовании государствами информационно-коммуникационных технологий (ИКТ) и норм, правил и принципов ответственного поведения государств.

Для поддержания международной стабильности чрезвычайно важно, чтобы государства ответственно использовали ИКТ и чтобы их использование поощрялось в качестве инструмента экономического и социального развития.

Колумбия выступает за свободный, открытый и безопасный Интернет и за то, чтобы страны располагали инструментами, позволяющими им эффективно сотрудничать в борьбе с киберпреступностью, наращивали свой национальный потенциал и усиливали меры укрепления доверия между странами.

Чрезвычайно важно признавать и решать вопросы, связанные с цифровой идентификацией личности, в частности такие, как сотрудничество с поставщиками интернет-услуг; цифровые доказательства, методы их получения и хранения, порядок передачи, сертификации и пригодности; защита данных, неприкосновенность частной жизни и уважение прав и свобод человека.

Однако мы полагаем, что обсуждение проблемы киберпреступности с технической и политической точек зрения следует продолжать главным образом в Комиссии по предупреждению преступности и уголовному правосудию через Межправительственную группу экспертов по киберпреступности, а не создавать новые альтернативные группы с ограниченным количеством стран-членов, например Группу правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности.

Колумбия хотела бы принимать участие в международных обсуждениях, проходящих в Рабочей группе открытого состава по достижениям в области информатизации и телекоммуникаций в контексте международной безопасности и в Межправительственной группе экспертов. В состав последней группы Колумбия выдвинула одного кандидата. Если мы не сможем участвовать в работе этой группы, мы будем вносить свой вклад через региональные консультативные

центры, предоставляемые для этих целей Организацией американских государств (ОАГ).

Замечания по резолюциям Генеральной Ассамблеи 73/266 о поощрении ответственного поведения государств в киберпространстве в контексте международной безопасности и 73/27 о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности

Правительство Колумбии согласно с тем, что необходимо улучшать координацию и сотрудничество между государствами в целях поощрения ответственного использования ИКТ государствами в качестве одного из основополагающих элементов обеспечения международной стабильности, а также для того, чтобы превратить ИКТ в реальный инструмент экономического и социального развития.

Колумбия активно участвовала в работе Межправительственной группы экспертов в 2014–2015 годах, когда был принят последний на тот момент документ по этому вопросу, и полностью согласна с содержащимися в нем концепциями, соображениями, толкованиями и рекомендациями.

Правительство Колумбии считает, что международное право должно применяться как к реальному, так и к виртуальному пространству. Этой позиции, или концепции, не только придерживаются эксперты Межправительственной группы экспертов, которые пришли к консенсусу относительно основных элементов ее применимости, — о ее важности свидетельствуют меры укрепления доверия, принимаемые Организацией по безопасности и сотрудничеству в Европе и Ассоциацией государств Юго-Восточной Азии, и Луккская декларация Группы семи об ответственном поведении государств в киберпространстве, а также единодушная поддержка группы экспертов по второй версии Таллинского руководства. В любом случае, необходимо продолжать изучение вопроса о применимости международного права к кибероперациям в целях прояснения неопределенностей или возможных расхождений в толковании его применения.

Менее развитым в технологическом отношении странам крайне важно заключать соглашения, которые предотвращали бы использование киберпространства как места развертывания конфликта, из-за возможных последствий, с которыми им придется столкнуться либо как объекту враждебных кибероперациий, либо как «марионеточному государству» ввиду недостаточного потенциала для принятия превентивных мер.

В менее развитых в технологическом отношении странах вмешательство в критически важную информационную инфраструктуру может иметь огромные последствия не только по причине зависимости от информационных технологий и перехода к автоматизации промышленных процессов с использованием интернет-технологий, но и из-за незнания рисков и угроз, а также из-за нехватки ресурсов, необходимых для укрепления цифровой безопасности компаний, отвечающих за эксплуатацию этой инфраструктуры.

Чрезвычайно важно вынести на самый высокий уровень обсуждение вопроса о том, что подразумевает Устав Организации Объединенных Наций, и его применимости в плане поддержания мира и стабильности, с тем чтобы содействовать созданию открытой, безопасной, стабильной, доступной и мирной ИКТ-среды.

Усилия, предпринимаемые на национальном уровне для укрепления информационной безопасности и содействия международному сотрудничеству в этой области, и проблемы на национальном уровне

В целях решения проблем, связанных с неопределенностями, рисками, угрозами, факторами уязвимости и инцидентами в киберпространстве, в 2011 году правительство страны опубликовало документ 3701 Национального совета по социально-экономической политике «Руководящие принципы политики в области кибербезопасности и киберзащиты». В соответствии с этой политикой страна уделяет основное внимание усилиям по противодействию росту киберугроз, которые оказывают на нее существенное влияние, и разработке нормативно-правовой и институциональной базы для решения проблем в области кибербезопасности. Ниже приводится общий обзор хода осуществления этих руководящих принципов политики и их пересмотра в 2014 и 2015 годах.

Общая цель документа 3701 заключалась в укреплении потенциала государства по противодействию угрозам национальной обороне и безопасности в киберпространстве (кибербезопасности и кибероборо не) и создании среды и условий для обеспечения защиты в киберпространстве. Для достижения этой общей цели были сформулированы три конкретные задачи: a) учредить надлежащие органы по предотвращению, координации, контролю и регулированию инцидентов или чрезвычайных ситуаций в компьютерной сфере и реагированию на них и разрабатывать рекомендации по устранению угроз и рисков, подрывающих национальную кибербезопасность и кибероборону; b) обеспечить специализированную подготовку по вопросам информационной безопасности и расширить направления исследований в области кибероборо ны и кибербезопасности; c) укрепить законодательство в области кибербезопасности и кибероборо ны и международное сотрудничество и ускорить присоединение Колумбии к различным международным документам в этой области.

В развитие этой политики и на основе новой концепции, базирующейся на передовой международной практике, в особенности с учетом принципов и рекомендаций таких многосторонних организаций, как Организация Североатлантического договора (НАТО), Организация экономического сотрудничества и развития, Международный союз электросвязи и ОАГ, и глобальных организаций частного сектора, которые проанализировали пути решения проблемы цифровой безопасности в нынешних условиях цифровой среды, в 2016 году правительство страны издало документ 3854 Национального совета по социально-экономической политике «Национальная стратегия в области цифровой безопасности», действующий до декабря 2019 года и имеющий своей целью расширение возможностей различных заинтересованных сторон по выявлению, смягчению, устранению рисков в области цифровой безопасности и управлению ими в своей социально-экономической деятельности в цифровой среде на основе сотрудничества, взаимодействия и помощи. Ожидается, что эта стратегия будет содействовать росту национальной цифровой экономики, что, в свою очередь, будет способствовать повышению экономического и социального благо состояния в стране.

Для достижения общей цели этой государственной стратегии были поставлены следующие конкретные задачи: a) создать институциональную базу в области цифровой безопасности, согласующуюся с подходом к управлению рисками; b) создать условия, позволяющие различным заинтересованным сторонам контролировать риски в области информационной безопасности в своей социально-экономической деятельности и укрепляющие доверие в вопросах использования цифровых технологий; c) повысить безопасность людей и государства в цифровой среде на национальном и транснациональном уровнях с упором на

управление рисками; d) укрепить национальную оборону и суверенитет в цифровой среде с упором на управление рисками; e) разработать постоянные и стратегические механизмы для содействия сотрудничеству, взаимодействию и помощи в области цифровой безопасности на национальном и международном уровнях.

Со времени принятия Национальным советом по социально-экономической политике в апреле 2016 года плана действий и контроля, сопровождающего национальную стратегию в области цифровой безопасности, компетентные государственные органы принимают меры, предусмотренные в этом плане, с тем чтобы достичь общей цели и выполнить конкретные задачи, поставленные в рамках этой стратегии.

В заключение в результате принятия предусмотренных мер были достигнуты следующие успехи:

- Начала создаваться скоординированная институциональная база с участием различных заинтересованных сторон в целях реализации национальной стратегии в области цифровой безопасности, в частности путем создания должности национального координатора по вопросам цифровой безопасности в канцелярии президента Республики и обеспечения бесперебойного функционирования Группы по реагированию на чрезвычайные ситуации в компьютерной сфере Колумбии.

- Начался процесс разработки и осуществления в рамках национального правительства модели управления рисками в области цифровой безопасности, учитывающей концептуальные рамки этой стратегии, международные стандарты безопасности и комплексную систему управления рисками на национальном уровне.

- Начали создаваться условия, позволяющие различным заинтересованным сторонам контролировать риски в области цифровой безопасности в своей социально-экономической деятельности и укрепляющие доверие в вопросах использования цифровых технологий, в частности проводится исследование по вопросу о воздействии киберпреступлений и правонарушений в стране и корректируется нормативная база в секторе ИКТ с целью повысить цифровую безопасность.

- Были разработаны планы по укреплению оперативного, административного, кадрового и научного потенциала и физической и технологической инфраструктуры учреждений, образующих часть действующей институциональной базы в рамках национального правительства.

- Были подписаны соглашения о международном сотрудничестве со странами-партнерами и важными представителями данной сферы, направленные на укрепление потенциала и содействие обмену информацией об угрозах. В 2017 году НАТО единогласно одобрила подписание индивидуальной программы сотрудничества и партнерства с Колумбией, которая стала первой латиноамериканской страной, получившей этот статус и заявившей о себе в качестве глобального партнера. Один из пунктов этого правового документа предусматривает совершенствование навыков в компьютерной сфере. По мнению Колумбии, необходимо укреплять существующие инициативы в различных сценариях в рамках Организации Объединенных Наций.

Что касается задачи создания институциональной базы для обеспечения цифровой безопасности в соответствии с подходом к управлению рисками, то следует отметить такие успехи, как создание должности национального

координатора по вопросам цифровой безопасности, обеспеченного техническими и правовыми средствами, и учреждение Комитета по цифровой безопасности, который будет предоставлять рекомендации по вопросам управления и выполнения государственных функций и действовать на высшем межведомственном и межсекторальном уровне национального правительства для обеспечения руководства по вопросам цифровой безопасности. Следует отметить также разработку таких ключевых инструментов, как модель управления рисками в области цифровой безопасности, которую национальные органы исполнительной власти обязаны принять и применить на практике и которую Административный департамент государственного управления в августе 2018 года включил в «Руководство по противодействию рискам, связанным с управлением, коррупцией и цифровой безопасностью, и разработке механизмов контроля в государственных учреждениях».

Среди вызовов, связанных с выполнением этой задачи, следует отметить необходимость внедрения и укрепления системы управления рисками в области цифровой безопасности в учреждениях, отвечающих за кибербезопасность и кибероборону и образующих часть создаваемой институциональной базы. Кроме того, необходимо укреплять секторальный потенциал, более эффективно поощряя и создавая секторальные группы по реагированию на чрезвычайные ситуации в компьютерной сфере, составить практичный план эффективного развертывания Комитета по цифровой безопасности, разработать эффективный протокол связи между секторальными и местными отделениями и национальными координационными центрами по вопросам цифровой безопасности, а также выявлять и оценивать риски со стороны всех многочисленных заинтересованных сторон и эффективно управлять ими.

Что касается второй задачи — создание условий, позволяющих различным заинтересованным сторонам контролировать риски в области информационной безопасности в своей социально-экономической деятельности и укрепляющих доверие в вопросах использования цифровых технологий, — то был достигнут определенный прогресс в деле разработки проекта национальной программы в области цифровой безопасности. Вместе с тем необходимо продолжать укреплять взаимосвязи между обсуждениями всех заинтересованных сторон, привлекать более весомый научный вклад (исследования) по данному вопросу и оказывать государственным учреждениям содействие в принятии модели управления рисками в области цифровой безопасности. Был проведен ряд информационно-просветительских кампаний, таких как программа «Я доверяю ИКТ»; кроме того, при поддержке ОАГ в 2017 году было подготовлено «Исследование об экономических последствиях инцидентов, угроз и кибератак в Колумбии», и такое же исследование готовится за 2018 год.

Что касается вызовов, то мы признаем, что необходимо определить направления исследований в области цифровой безопасности, которые следует продолжать и укреплять; установить четкую и эффективную модель координации и коммуникации, которая позволит создать необходимую правовую основу в области цифровой безопасности, способствующую цифровой трансформации различных заинтересованных сторон; эффективно распространять информацию о результатах стратегических исследований на высоких уровнях правительства для принятия решений; и переориентировать стратегию создания учебных материалов, подлежащих включению в учебные программы на различных уровнях образования.

Что касается третьей задачи — повысить безопасность людей и государства в цифровой среде на национальном и транснациональном уровнях с упором на управление рисками, — то был достигнут прогресс в разработке планов по

укреплению потенциала ключевых органов, подготовке докладов по статистике киберпреступлений и наращивании потенциала в области управления рисками органов, отвечающих за кибербезопасность в стране.

Одним из вызовов, связанных с выполнением этой задачи, является насущная потребность в реализации планов по укреплению оперативного, административного, кадрового и научного потенциала и физической и технологической инфраструктуры, предназначенных для органов и структур, отвечающих за кибербезопасность, а также в определении руководящих принципов адаптации существующей нормативно-правовой базы к потребностям в следующих сферах: a) анализ, прогнозирование, предупреждение, выявление, расследование правонарушений, преступлений и явлений в киберпространстве и правонарушений и преступлений с использованием цифровой среды и реагирование на них; b) преследование за совершение и криминализация новых видов преступлений, включающих компьютерные преступления, совершенные в целях отмывания денег; c) функционирование государственных органов безопасности, обороны и разведки в цифровой среде в соответствии с основополагающими принципами национальной политики в области цифровой безопасности.

Что касается четвертой задачи — укрепление национальной обороны и суверенитета в цифровой среде с упором на управление рисками, — то был достигнут прогресс в разработке планов по укреплению потенциала ключевых учреждений, в периодическом обновлении каталога национальных критически важных киберинфраструктур, в создании некоторых компонентов планов защиты критически важной киберинфраструктуры, в создании ряда секторальных групп реагирования на инциденты кибербезопасности в целях содействия надлежащему реагированию на такие инциденты в национальных критически важных киберинфраструктурах (например, правительства, финансового сектора и энергетики), а также в участии некоторых заинтересованных сторон в практических и теоретических учениях, проводимых на национальном и международном уровнях в целях развития навыков и способностей различных заинтересованных сторон, отвечающих за безопасность ключевых национальных киберинфраструктур и национальную оборону в цифровом пространстве.

Для выполнения этой задачи необходимо переориентировать, с самого высокого уровня, руководящие принципы защиты и обороны важнейших национальных киберинфраструктур с учетом новых условий и официально издать протокол по управлению инцидентами в области цифровой безопасности, направленными на объекты этого типа инфраструктуры, и реагированию на них. Кроме того, необходимо разработать стратегию, в рамках которой правительство страны объединит усилия по повышению осведомленности и подготовке в сфере цифровой безопасности в том, что касается национальной обороны.

Наконец, что касается пятой задачи, связанной с разработкой постоянных и стратегических механизмов для содействия сотрудничеству, взаимодействию и помощи в области цифровой безопасности на национальном и международном уровнях, то был достигнут прогресс в применении механизмов содействия сотрудничеству, взаимодействию и помощи на международном уровне в области цифровой безопасности. Следует отметить также успехи, достигнутые в процессе присоединения к Конвенции о киберпреступности и в подготовке проекта стратегической программы в области международного сотрудничества, взаимодействия и помощи.

Что касается вызовов, связанных с выполнением этой задачи, то необходимо определить ситуации, в которых Колумбия должна была бы участвовать в решении вопросов цифровой безопасности, и уделить им приоритетное внимание, а также установить четкую и эффективную модель координации и

коммуникации между заинтересованными сторонами, которая позволит разрабатывать и исполнять стратегические документы, способствующие развитию сотрудничества, взаимодействия и помощи в вопросах цифровой безопасности как на национальном, так и на международном уровнях.

С учетом вышесказанного и ввиду того, что национальная политика в сфере цифровой безопасности, изложенная в документе 3854 Национального совета по социально-экономической политике 2016 года, предусматривает план действий на период до 2019 года, правительство страны при поддержке ОАГ разрабатывает новую стратегию, для того чтобы справиться с вышеупомянутыми вызовами.

Куба

[Подлинный текст на испанском языке]
[29 апреля 2019 года]

Новые информационно-коммуникационные технологии (ИКТ) должны использоваться мирно в интересах всеобщего блага человечества и дальнейшего устойчивого развития всех стран вне зависимости от их научного и технологического развития.

Такие научно-технические достижения могут иметь как гражданское, так и военное применение, при этом прогресс не должен сказываться на международной безопасности государств.

Единственным способом, позволяющим избежать превращения киберпространства в театр военных действий, является широкое сотрудничество между всеми государствами.

В этой связи мы поддерживаем учреждение Рабочей группы открытого состава по достижениям в области информатизации и телекоммуникаций в контексте международной безопасности в соответствии с резолюцией 73/27 Генеральной Ассамблеи с целью придания процессу переговоров Организации Объединенных Наций по безопасности при использовании ИКТ более демократического, инклюзивного и транспарентного характера.

Мы считаем, что следует создать юридически обязательную международную нормативно-правовую базу, которая дополняла бы существующие нормы международного права и была бы применима к ИКТ.

Все государства обязаны уважать существующие международные стандарты в этой сфере. Доступ к информационным или телекоммуникационным системам другого государства должен осуществляться с соблюдением международных соглашений о сотрудничестве на основе принципа согласия соответствующего государства. Формы и масштабы обмена должны определяться на основе уважения законодательства того государства, к системе которого открывается доступ.

Использование телекоммуникаций во враждебных целях с явным или тайным намерением подорвать правовые и политические системы государств является нарушением норм, признанных на международном уровне в этом отношении, и представляет собой незаконное и безответственное использование этих средств.

С помощью незаконных радио- и телепередач совершаются постоянные вторжения в информационное пространство Кубы, а также распространяются

программы, специально предназначенные для подстрекательства к свержению конституционного строя, установленного кубинским народом.

На протяжении 2018 года с территории Соединенных Штатов велось незаконное вещание на Кубу в среднем в течение 1653 часов в неделю на 20 частотах, что идет вразрез с целями и принципами Устава Организации Объединенных Наций, международного права и положений Международного союза электросвязи.

Куба вновь призывает к немедленному прекращению этой агрессивной политики, наносящей ущерб ее суверенитету и, помимо всего прочего, несовместимой с налаживанием отношений между государствами на основе взаимного уважения и сотрудничества.

Экономическая, торговая и финансовая блокада, введенная правительством Соединенных Штатов в отношении Кубы почти 60 лет назад, наносит серьезный ущерб кубинскому народу, в том числе в плане пользования ИКТ.

На второй Встрече на высшем уровне глав государств и правительств Сообщества государств Латинской Америки и Карибского бассейна (СЕЛАК) главы государств и правительств стран Латинской Америки и Карибского бассейна провозгласили этот регион зоной мира и, среди прочего, обязались укреплять сотрудничество и дружественные отношения между собой и с другими государствами вне зависимости от различий в их политических, экономических и социальных системах или уровнях развития, проявлять терпимость и жить вместе, в мире друг с другом, как добрые соседи.

На пятой Встрече на высшем уровне глав государств и правительств СЕЛАК, состоявшейся в январе 2017 года в Пунта-Кане (Доминиканская Республика), вновь была подчеркнута важность ИКТ, включая Интернет, в качестве средств поощрения мира, благосостояния человечества, развития, обмена знаниями, социальной интеграции и экономического роста.

Египет

[Подлинный текст на английском языке]
[9 мая 2019 года]

Введение

За последние 30 лет в мире резко увеличились масштабы использования Интернета, смартфонов и современных устройств информационно-коммуникационных технологий (ИКТ); ошеломляюще часто ИКТ стали использоваться в таких областях, как бизнес, торговля, государственные услуги, образование, передача знаний, развлечения, туризм, здравоохранение, и в других видах экономической, социальной и культурной деятельности. Наряду с возможностями, открывающимися в результате непрерывного расширения масштабов использования телекоммуникаций и Интернета и стремительного перехода на электронные операции и электронные услуги, важно различать вызовы и угрозы, объектами которых становятся инфраструктура ИКТ и электронные операции в целом, и противостоять им, поскольку они подрывают доверие к электронным услугам и электронному бизнесу в частности.

В этой связи Египет придает огромное значение той важной роли, которую играют разработка и применение новейших информационных технологий и средств телекоммуникаций в достижении экономического и социального прогресса как на национальном, так и на международном уровне. Египет активно поддерживает также использование ИКТ на общее благо человечества и в целях

содействия устойчивому развитию всех стран, независимо от уровня их научно-технического прогресса. Кроме того, Египет полагает, что Организация Объединенных Наций должна играть главную роль в руководстве соответствующими международными усилиями и содействии диалогу между государствами-членами в целях выработки общего международного понимания того, как применяются нормы международного права, правила и принципы, касающиеся ответственного поведения государств в сфере информатизации, включая исполнение юридически обязательных документов.

Наиболее серьезные киберугрозы

1. Угроза проникновения в инфраструктуру ИКТ и ее саботажа

В последнее время появились новые виды чрезвычайно серьезных кибератак, направленных на то, чтобы подорвать работу основных служб и установить вредоносные программы и вирусы, которые разрушают или нарушают работу инфраструктуры ИКТ и критически важных автоматизированных систем управления, особенно на таких ключевых объектах, как ядерные, нефтегазовые и энергетические установки, авиация, различные виды транспорта, важнейшие национальные базы данных, государственные службы, здравоохранение и службы неотложной помощи. В ходе таких кибератак используется несколько каналов, включая беспроводные сети и мобильные устройства памяти, и другие общие каналы, такие как электронная почта, веб-сайты, социальные сети и телекоммуникационные сети, от которых может в значительной степени зависеть использование критически важных объектов инфраструктуры и связанных с ними служб и предприятий. На практике ключевые объекты могут быть уязвимы перед лицом изощренных кибератак, даже не будучи напрямую подключенными к Интернету.

2. Угроза кибертерроризма и кибервойны

В последнее время получили распространение опасные виды кибератак и киберпреступлений с использованием таких передовых технологий, как облачные вычисления, прослушивание, вторжение в сеть и шифрование с использованием продвинутых стандартов, и автоматизированных хакерских инструментов для взлома компьютерных систем и баз данных. Кроме того, злоумышленники могут устанавливать продвинутое вредоносное программное обеспечение (вредоносные программы), с тем чтобы пробить брешь в системах защиты сети и компьютерных системах и создать бот-сети, которые впоследствии могут использоваться в разного рода преступной и незаконной деятельности. Автоматизированная бот-сеть может состоять из десятков, сотен тысяч или миллионов взломанных компьютеров, которые могут быть использованы для осуществления серьезных кибератак, таких как распределенная атака «отказ в обслуживании», на сети и веб-сайты в целях разрушения, терроризма и/или вымогательства.

Для разработки сложных и изощренных компьютерных вирусов, предназначенных для использования в тактических, стратегических и военных целях, а также в дополнение к обычным военным атакам, а иногда и вместо них, в ходе так называемой кибервойны, зачастую требуется высокий уровень знаний и нетрадиционный опыт, доступные только в технически развитых странах. Однако такие вредоносные технологии передаются, копируются или воспроизводятся террористическими организациями, которые используют их в террористических операциях и организованных преступлениях, а также для того, чтобы создать угрозу инфраструктурам ИКТ и нарушить их работу в целях вымогательства и/или промышленного шпионажа. Египет подтверждает выводы ведущих

экспертов в сфере кибербезопасности о том, что в предстоящий период ожидается увеличение числа ожесточенных и изощренных кибератак.

3. Угроза хищения цифровых идентификационных и конфиденциальных данных

Хищение цифровых идентификационных данных является одним из наиболее серьезных преступлений, угрожающих пользователям Интернета и будущему электронных услуг. Украденные регистрационные и личные данные могут использоваться преступниками для того, чтобы выдавать себя в киберпространстве за других с целью присвоить себе деньги и имущество или очернить имена жертв в связи с подозрительной или незаконной деятельностью. Преступник, крадущий личные данные, обычно использует информацию, которая уже имеется в Интернете, в частности в открытых социальных и профессиональных сетях, национальных базах данных, сетях государственных служб, служб социального обеспечения и здравоохранения, сетях электронных платежей, банкоматах и на веб-сайтах электронной торговли, виртуальных рынках и фондовых биржах. Кроме того, инструменты и системы, используемые при проведении электронных операций, могут быть скомпрометированы, украдены или повреждены, что создает серьезную угрозу интересам пользователей и будущему электронных услуг. Объектом продолжительных и широкомасштабных кибератак может стать национальный финансовый сектор. Результатом хищения данных государственных учреждений и компаний могут стать значительные материальные потери, потеря доверия, ущерб репутации, отток клиентов и снижение стоимости нематериальных активов, что может отрицательно сказаться на национальной экономике в целом.

Основные причины серьезности новых киберугроз

Новые киберугрозы могут иметь очень серьезные последствия по трем нижеперечисленным причинам.

1. Они зачастую связаны с применением современных передовых технологий, монополией на которые, как правило, обладают высокоразвитые страны и крупные компании. Многие из этих технологий являются сверхсекретными и недоступными для экспорта. При этом экспортируемые версии некоторых технологий могут содержать дефекты или уязвимости, которые делают их источником дополнительных угроз.

2. В ходе кибератак могут легко и быстро распространяться вредоносные вирусы, осуществляться распределенные атаки «отказ в обслуживании» и другие изощренные кибератаки ввиду широкого применения ИКТ, а также потому, что произвести дистанционный запуск таких атак и передачу вирусов через границы из любой точки мира просто и дешево. Кроме того, вовремя установить основной источник этих угроз и рисков в целях их устранения и преодоления трудно и зачастую невозможно.

3. Последствия кибератак могут быть весьма масштабными; так, они могут оказывать значительное прямое и косвенное воздействие на инфраструктуру, нанося существенный ущерб и причиняя значительные убытки. Кроме того, они могут осуществляться дистанционно и внезапно и непредсказуемо приобретать большой масштаб, потенциально оказывая негативное воздействие на критически важные организации и огромные числа людей, измеряемые в тысячах или даже миллионах.

Путь вперед: как противостоять киберугрозам

Кибератаки и киберпреступления не ограничиваются географическими пределами стран и, как правило, осуществляются при помощи как традиционных, так и технических сетей организованной преступности. Поэтому методы противодействия таким нападениям и преступлениям должны включать традиционные механизмы международного сотрудничества, направленные на борьбу с преступностью и киберугрозами, а также законодательную и нормативную базу, предусматривающую специальные механизмы для реагирования на новые технические разработки. Для эффективного реагирования на кибератаки и киберпреступления требуются сотрудничество и координация на национальном уровне между партнерами, предоставляющими и эксплуатирующими инфраструктуру в ключевых секторах, и партнерами, предоставляющими услуги, включая государственные учреждения, институты и компании. Кроме того, огромное значение имеют международные и региональные сотрудничество и координация, в которые должны быть вовлечены ключевые международные организации, региональные объединения и профессиональные и специализированные международные форумы.

Вклад Египта

Египет осознает важность международного сотрудничества в решении проблем кибербезопасности. Египетские эксперты вносят свой вклад в работу ряда соответствующих правительственных групп экспертов, которым Генеральная Ассамблея поручила выработать согласованные рекомендации в отношении кибербезопасности с точки зрения международной безопасности. Кроме того, в качестве члена Международного союза электросвязи (МСЭ) Египет входил в состав его Группы экспертов высокого уровня по кибербезопасности и принимал участие в деятельности Группы в рамках Глобальной программы кибербезопасности. Кроме того, Египет предложил создать Рабочую группу Совета МСЭ по защите детей в Интернете и председательствовал в ней с 2010 по 2017 год. Египет также принимает участие в региональных конференциях, семинарах и практикумах по кибербезопасности, организуемых такими международными организациями, как МСЭ, Организация исламского сотрудничества, Организация по безопасности и сотрудничеству в Европе, Организация экономического сотрудничества и развития и Форум центров компьютерной безопасности и реагирования на компьютерные инциденты, и является их принимающей стороной. Помимо этого, Египет участвует в международных и региональных исследованиях в области кибербезопасности совместно с такими профессиональными организациями, как Ассоциация Глобальной системы мобильной связи. Кроме того, Египет принимает активное участие в региональных усилиях в африканских и арабских странах с целью содействовать усилиям по обеспечению транспарентности в деле укрепления доверия и наращивания потенциала и распространению передовой практики. Египет также выступает одной из сторон в двусторонних консультациях и переговорах с рядом государств и международных организаций и партнеров в целях заключения соглашений о двустороннем сотрудничестве в этой стратегической области.

На национальном уровне в соответствии со статьей 31 Конституции Египта в конце 2014 года на уровне кабинета министров был создан Высший совет по защите критически важной информационной инфраструктуры и кибербезопасности (Высший совет кибербезопасности Египта). Председателем Совета является министр коммуникаций и информационных технологий, а его членами являются представители важнейших секторов и ключевых органов безопасности. На оперативном уровне техническим органом Совета стала национальная Группа реагирования на компьютерные инциденты. В 2017 году Совет

разработал первую национальную стратегию Египта в сфере кибербезопасности. Масштабы, структура и цели этой стратегии соответствуют национальным требованиям и международным нормам, правилам и принципам. Реализация стратегии происходит в том же духе.

Заключение

Египет вновь заявляет о настоятельной необходимости активизировать усилия по наращиванию потенциала развивающихся стран и оказанию им технической помощи в области безопасности ИКТ, особенно с учетом того, что прочность системы кибербезопасности нередко определяется степенью прочности ее самого слабого звена.

Кроме того, результативная работа Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и подготовленные в итоге соответствующие доклады, препровожденные Генеральным секретарем Генеральной Ассамблее, представляют собой важные шаги в нужном направлении. Главным из них является подчеркивание исключительной важности того, чтобы государства были привержены принципам Устава Организации Объединенных Наций и другим принципам международного права, включая суверенное равенство; принципу разрешения международных споров мирными средствами; отказа в международных отношениях от угрозы силой или ее применения как против территориальной неприкосновенности или политической независимости любого государства, так и каким-либо другим образом, несовместимым с целями Организации Объединенных Наций; принципу уважения прав человека и основных свобод; и принципу невмешательства во внутренние дела других государств. Конечная цель заключается в создании надежной и безопасной информационно-коммуникационной среды, исходя из необходимости сохранить свободное распространение информации.

В свете серьезности возникающих киберугроз Египет высоко ценит и поддерживает содержащуюся в резолюции 73/27 рекомендацию о создании рабочей группы открытого состава, действующей на основе консенсуса, в целях продолжения в качестве приоритета дальнейшей выработки норм, правил и принципов ответственного поведения государств для придания переговорному процессу в Организации Объединенных Наций по безопасности в сфере использования информационно-коммуникационных технологий более демократического, инклюзивного и транспарентного характера. Кроме того, Египет рассчитывает присоединиться к усилиям этой рабочей группы открытого состава по разработке методов осуществления таких правил, норм и мер укрепления доверия и поддержать их.

Египет также рассчитывает на участие в работе Группы правительственных экспертов, учрежденной резолюцией 73/266, в том числе в ее деятельности по налаживанию сотрудничества с соответствующими региональными организациями в процессе консультаций.

Франция

[Подлинный текст на французском языке]
[14 мая 2019 года]

1. Общая оценка вопросов кибербезопасности

В предварительном порядке Франция хотела бы отметить, что она не использует термин «информационная безопасность», отдавая предпочтение термину «безопасность информационных систем», или «кибербезопасность». Это обусловлено тем, что Франция, будучи активной поборницей свободы выражения мнений в интернете (о чем свидетельствует тот факт, что в 2018 году она была соавтором резолюции 38/7 Совета по правам человека), не считает, что сама по себе информация может быть фактором уязвимости, от которого необходимо защищать себя, без ущерба для мер, которые могут быть приняты на пропорциональной и транспарентной основе в условиях, строго определенных правовыми рамками, в соответствии со статьей 19 Международного пакта о гражданских и политических правах.

Термин «кибербезопасность» является более точным, поскольку он означает способность информационной системы противостоять явлениям из киберпространства, которые ставят под угрозу доступность, целостность и конфиденциальность хранящихся, обрабатывающихся или передающихся данных и связанных с ними услуг, которые имеются в этих системах или к которым эти системы обеспечивают доступ. Кибербезопасность основывается на методах обеспечения безопасности информационных систем и поддерживается за счет борьбы с киберпреступностью и создания системы киберзащиты.

Франция считает, что цифровое пространство должно оставаться областью свободы, взаимодействия и роста, обуславливающей процветание и прогресс в обществе. Как она уже подчеркивала в 2015 году в своей национальной стратегии цифровой безопасности[1], Франция считает, что «цифровые технологии, несущие в себе новые форматы использования и новые услуги, являются движущей силой инноваций. Они приводят к изменениям в большинстве профессий. Они меняют сферы деятельности и компании, привнося гибкость и конкурентоспособность». Они дают членам общества возможность упростить повседневную деятельность с помощью коммуникационных, торговых и информационных онлайн-услуг, а также обеспечивают экономические возможности за счет усиления конкуренции или развития коллаборативной экономики.

В настоящее время это открытое, защищенное, стабильное, доступное и мирное киберпространство, которое предоставляет экономические, политические и социальные возможности, поощряемые Францией на протяжении последних 30 лет, находится под угрозой из-за новых разрушительных тенденций, появившихся в киберпространстве. Это связано с тем, что специфика цифрового пространства (относительная анонимность, низкая стоимость, простота доступа к вредоносным программам, легкость внедрения, скорость распространения факторов уязвимости и так далее) нередко позволяет создать цифровой арсенал, который можно использовать для шпионажа, незаконного оборота, дестабилизации и саботажа. Несмотря на то, что некоторые низкоуровневые угрозы являются не вопросом национальной безопасности, а формой преступности, применение кибернетического оружия против государственных систем обработки данных, объектов критически важной инфраструктуры или крупных компаний может иметь серьезные последствия.

[1] URL: www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf.

В настоящее время вопросы кибербезопасности являются неотъемлемой частью силовых стратегий, определяющих баланс сил и международные отношения; это приоритетная и первостепенная политическая проблема. Как подчеркивается в стратегическом обзоре обороны и национальной безопасности за 2017 год[2], «произошедшая за последнее десятилетие массовая цифровизация наших обществ и глобальная взаимосвязь информационно-коммуникационных систем создают как новые угрозы, так и новые возможности. Они обеспечивают всеобщий доступ к эффективным инструментам выражения мнений, влияния, пропаганды и распространения информации, к огромным массивам данных, но также к устрашающим способам нападения. Они способствуют появлению новых участников из числа представителей частного сектора, которые перехватывают инициативу на международной арене, бросая вызов суверенитету государств, но также и выступая порой в качестве важных партнеров. По сути, они меняют баланс в распределении полномочий между государственными, негосударственными и частными субъектами».

Мы все несем ответственность за сохранение, развитие и поддержку открытого, безопасного, стабильного, доступного и мирного киберпространства. Столкнувшись с общими угрозами международной стабильности и безопасности, Франция вот уже несколько лет принимает активные политические и дипломатические меры, направленные на укрепление безопасности, доверия и стабильности в киберпространстве.

2. Усилия по укреплению национальной кибербезопасности и содействию международному сотрудничеству в этой области

a) Совершенствование французских механизмов обеспечения кибербезопасности

Обеспечение кибербезопасности по-прежнему является одной из приоритетных задач деятельности правительства, заявленных в руководящих принципах, утвержденных в недавние годы во Франции на самом высоком государственном уровне.

Франция продолжает развивать и совершенствовать свои национальные механизмы. Опираясь на меры, принятые за последние десять лет (работа по созданию и укреплению потенциала Национального агентства по безопасности систем информации, которая ведется с 2009 года; разработка первой французской стратегии защиты и безопасности информационных систем в феврале 2011 года; укрепление правовых инструментов и существенное увеличение ресурсов, выделяемых на кибербезопасность в соответствии с последними законами о военном планировании; публикация Министерством вооруженных сил в феврале 2014 года «Соглашения по киберзащите»; и создание центра кибертехнологий в целях стимулирования развития образовательного и научно-исследовательского компонента и промышленно-технологической базы в области кибербезопасности), она проводит также политику транспарентности в отношении своей стратегии как на национальном, так и на международном уровне.

Так, в 2015 году для поддержки переходного периода цифровизации французского общества Франция приняла национальную стратегию обеспечения цифровой безопасности. С точки зрения безопасности в ней подчеркивается необходимость принятия решительных мер по борьбе с киберпреступлениями и ставится цель превратить цифровую безопасность в конкурентное преимущество французских компаний.

[2] URL: www.defense.gouv.fr/dgris/presentation/evenements-archives/revue-strategique-de-defense-et-de-securite-nationale-2017.

В декабре 2017 года этот документ был дополнен международной стратегией Франции в области цифровых технологий, в которой были изложены конкретные принципы и цели Франции в отношении этой области на международном уровне[3]. Эта стратегия включает три основных компонента (управление, экономика и безопасность) и направлена на:

- содействие формированию открытого, разнообразного и способствующего укреплению доверия цифрового мира в глобальном масштабе;
- утверждение европейской модели баланса между экономическим ростом, основными правами и свободами и безопасностью;
- укрепление влияния, привлекательности, безопасности и торговых позиций Франции и французских субъектов в цифровом мире.

В представленном в феврале 2018 года стратегическом обзоре киберзащиты[4] определена концепция регулирования кибернетических кризисных ситуаций и уточнены национальные стратегические цели в области киберзащиты. Эта концепция, в которой подтверждается актуальность французской модели и возложенная на государство главная ответственность в области кибербезопасности, опирается на следующие семь основных принципов:

- повышение защищенности информационных систем нашей страны;
- сдерживание атак путем принятия комплекса мер защитного характера, повышения сопротивляемости и усиления потенциала реагирования и принятия ответных мер;
- подтверждение и осуществление цифрового суверенитета Франции;
- повышение эффективности реагирования системы уголовного правосудия на киберпреступления;
- повышение общей культуры информационной безопасности;
- участие в становлении безопасной цифровой Европы, способствующей укреплению доверия;
- осуществление международной деятельности по содействию коллективному и контролируемому регулированию киберпространства.

Закон о военном планировании на 2019–2025 годы[5] предусматривает, по сравнению с предыдущими законами, значительное увеличение ресурсов, выделяемых на киберзащиту, в частности в области людских ресурсов, с целью набора 1500 дополнительных сотрудников для доведения к 2025 году численности персонала, занимающегося этими вопросами в Министерстве вооруженных сил, до 4000 человек.

Эффективности французских технических и оперативных механизмов способствуют следующие субъекты:

- Национальное агентство по безопасности информационных систем, которое отвечает за предотвращение (включая нормативные документы) чрезвычайных ситуаций в области информационной безопасности в отношении государства и стратегических предприятий и организаций и реагирование на них. В настоящее время в нем работает 600 человек, и оно продолжает

[3] URL: www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf.

[4] URL: www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf.

[5] URL: www.legifrance.gouv.fr/eli/loi/2018/7/13/ARMX1800503L/jo/texte.

расти. Оно зарекомендовало себя в качестве источника определения соответствующих стандартов кибербезопасности;

- на Министерство вооруженных сил возложена двойная задача: защита сетей, обеспечивающих его деятельность, и тесная интеграция операций в киберпространстве в военную деятельность. В целях укрепления деятельности Министерства в этой области в сентябре 2017 года был назначен командир формирования киберзащиты, подчиняющийся начальнику штаба вооруженных сил. В этой связи в начале 2019 года Министерство вооруженных сил опубликовало стратегию оборонительной политики в области информационной безопасности, и одновременно с этим начальник штаба вооруженных сил впервые публично изложил концепцию наступательной политики в области информационной безопасности для военных операций;
- в задачи Министерства внутренних дел и Министерства юстиции входит борьба со всеми формами киберпреступности, при этом особое внимание уделяется национальным учреждениям и интересам, хозяйствующим субъектам и государственным органам, а также отдельным лицам.

b) Содействие международному сотрудничеству в целях обеспечения стабильности и безопасности киберпространства

Одной из приоритетных задач Франции является укрепление стратегической стабильности и международной безопасности в киберпространстве. Как отмечается в стратегическом обзоре киберзащиты, «сотрудничество международного сообщества в киберпространстве является эффективным способом повышения стабильности за счет обмена знаниями друг о друге и укрепления взаимного доверия между участниками, а также создания совместных механизмов урегулирования кризисов, коммуникации и деэскалации». Деятельность Франции по содействию международному сотрудничеству в вопросах кибербезопасности осуществляется в европейских и международных рамках.

Предотвращение кризисов путем расширения сотрудничества и наращивания потенциала

Франция считает, что основная цель ее деятельности в цифровом пространстве — это предотвращение кризисов. Таким образом, как подчеркивается в стратегическом обзоре киберзащиты, «укрепление защиты, устойчивости и сотрудничества всех субъектов киберпространства является прямым вкладом в укрепление нашей национальной безопасности». Для достижения этой цели необходимо укреплять техническое, оперативное и структурное сотрудничество с государствами-партнерами и международными организациями в целях развития глобальной устойчивости киберпространства и соответствующего потенциала этих различных субъектов.

Франция считает, что в силу большой взаимосвязанности сетей и обществ кибербезопасность для всех будет обеспечена только тогда, когда у каждого государства появится достаточный потенциал для защиты своих собственных информационных систем. Поэтому она работает над укреплением потенциала своих партнеров в области кибербезопасности в рамках двусторонних или многосторонних инициатив. Кроме того, такие инвестиции в сотрудничество выгодны всем сторонам, поскольку они позволяют нам быть проводниками новейших достижений, взаимодействуя с нашими партнерами и учась у них, делясь знаниями и опытом и укрепляя доверие между вовлеченными сторонами.

На техническом уровне Национальное агентство по безопасности информационных систем продолжает налаживать партнерские отношения с

аналогичными учреждениями во многих странах в целях содействия обмену важными данными, такими как информация об уязвимости или слабых сторонах продуктов и услуг. Кроме того, действующий при Агентстве Правительственный центр мониторинга, оповещения и реагирования на компьютерные атаки активно участвует в работе нескольких многосторонних сетей (Форум групп оперативного реагирования и обеспечения безопасности, Общеевропейская структура групп реагирования на инциденты информационной безопасности, Европейское объединение правительственных групп реагирования на инциденты информационной безопасности, Сеть групп реагирования на инциденты информационной безопасности Европейского союза), через которые он поддерживает контакты с группами реагирования на инциденты информационной безопасности во всем мире.

Что касается оперативного и структурного сотрудничества, то Франция проводит активную политику. В последние годы Франция направляла международных технических экспертов по кибербезопасности для работы в силах внутренней безопасности стран-партнеров. Франция также продолжает сотрудничать с Сенегалом в работе Национальной школы кибербезопасности, которая была открыта в Дакаре в конце 2018 года и деятельность которой направлена на решение региональных задач. Этот проект направлен на обеспечение краткосрочной и легко адаптируемой подготовки специалистов по кибербезопасности и старших должностных лиц в первую очередь из Западной Африки.

Что касается Европейского союза, то в целях укрепления киберустойчивости в европейском пространстве Франция вносит вклад в разработку добровольной рамочной программы сотрудничества в области предотвращения и урегулирования инцидентов. Это включает, в частности, разработку общих оперативных стандартов и процедур сотрудничества между партнерами, проверенных в ходе общеевропейских испытаний. Франция участвовала также в разработке «кибер-инструментария», который обеспечивает набор мер для европейского совместного дипломатического реагирования на компьютерные атаки с использованием мер по профилактике, взаимодействию и стабилизации.

Кроме того, Франция приняла активное участие в принятии европейских нормативных актов, учитывающих необходимость обеспечивать конкурентоспособность и использовать потенциал цифровых технологий и при этом обеспечивающих защиту граждан, компаний и государств-членов (право на конфиденциальность и защиту личных данных, защита критически важной инфраструктуры, борьба с террористическим контентом в интернете). Об этом свидетельствует принятие постановления (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 года о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных, директивы (ЕС) 2016/1148 Европейского парламента и Совета от 6 июля 2016 года о мерах по обеспечению повсеместно высокого уровня безопасности сетей и информационных систем в Европейском союзе и предстоящего вступления в силу постановления (ЕС) 2019/881 Европейского парламента и Совета от 17 апреля 2019 года о работе Агентства Европейского союза по кибербезопасности и о сертификации кибербезопасности информационно-коммуникационных технологий, которое заменит собой постановление (ЕС) № 526/2013 (постановление о кибербезопасности). Франция также активно поддерживает принятие европейского постановления, направленного на предотвращение распространения террористического контента в интернете и предъявление общих требований к интернет-провайдерам.

Наконец, Франция прилагает все усилия к тому, чтобы промышленная политика Европейского союза поддерживала ведение передовой научно-

исследовательской деятельности в целях содействия внедрению надежных и проверенных технологий и услуг в области цифровой безопасности.

На состоявшемся в июне 2016 года Варшавском саммите Организации Североатлантического договора (НАТО) союзные державы по инициативе Франции приняли обязательство в отношении киберзащиты. Это обязательство позволяет обеспечить выделение каждым государством — членом Североатлантического союза соответствующей доли ресурсов на укрепление своего потенциала киберзащиты и тем самым повысить общий уровень безопасности для всех. В мае 2018 года Франция приняла у себя первую конференцию, посвященную этому обязательству. Союзные державы также признали киберпространство районом операций, требующим защиты НАТО в той же мере, что и наземное, воздушное и морское пространство.

Предотвращение кризисов путем разработки стандартов, регулирующих поведение субъектов в киберпространстве

Франция считает, что непременным условием создания коллективной системы кибербезопасности является сбалансированность, основанная на нормах международного права. Кроме того, как подчеркивается во французской международной цифровой стратегии, Франция придает большое значение продолжению «диалога на основе сотрудничества со всеми заинтересованными частными и государственными субъектами и всеми международными партнерами, которые готовы к такому диалогу, как на двусторонней, так и на многосторонней основе».

Франция активно участвовала в переговорах, проводившихся под эгидой Организации Объединенных Наций в ходе последних пяти совещаний Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Она будет продолжать участвовать в возобновлении обсуждений как в Группе правительственных экспертов, так и в рабочей группе открытого состава в целях продвижения своей концепции цифрового пространства как области свободы, взаимодействия и роста, обуславливающей процветание и прогресс в обществе. Она также участвует в других международных форумах, где рассматриваются эти вопросы безопасности цифрового пространства.

В 2006 году Франция ратифицировала Конвенцию о киберпреступности, которая обеспечивает правовую основу для определения различных правонарушений в сфере противодействия киберпреступности и предусматривает гибкие и современные средства международного сотрудничества в этой области (например, создание круглосуточной сети для ускорения процедур оказания помощи между государствами-участниками). В настоящее время Франция выступает за универсализацию Конвенции, участниками которой на данный момент являются 63 государства, представляющие все континенты. Она активно участвует в переговорах по второму дополнительному протоколу к ней, который направлен на дальнейшее укрепление международного сотрудничества в этой области путем развития сотрудничества между органами полиции и взаимопомощи в уголовных делах, включая предоставление доступа к электронным доказательствам. Франция также поддерживает работу Группы экспертов по углубленному исследованию киберпреступности, подтверждающую центральную роль Управления Организации Объединенных Наций по наркотикам и преступности в этой области.

Парижский призыв к укреплению доверия и безопасности в киберпространстве[6], представленный президентом Французской Республики на Форуме по вопросам регулирования Интернета, состоявшемся 12 ноября 2018 года в Организации Объединенных Наций по вопросам образования, науки и культуры, отражает активную роль Франции в содействии созданию безопасного, стабильного и открытого киберпространства. Целью этого документа, который на сегодняшний день поддерживает 66 стран и около 500 негосударственных организаций, является поощрение некоторых фундаментальных принципов регулирования цифрового пространства, таких как применение международного права и прав человека в киберпространстве, ответственное поведение государств, государственная монополия на законное насилие и признание конкретных обязанностей частных субъектов.

Франция также участвует в деятельности Организации экономического сотрудничества и развития (ОЭСР). В декабре 2018 года она участвовала в организации первого совещания Глобального форума ОЭСР по цифровой безопасности в интересах процветания, посвященного ответственности частных субъектов в области цифровой безопасности.

Созданная в 2016 году в рамках Группы семи (Г-7) исэ-симская группа по кибервопросам, приняла в 2017 году амбициозную декларацию, известную как «Луккская декларация», о стандартах ответственного поведения государств в киберпространстве. В марте 2019 года в рамках своего председательства Франция предложила создать механизм контроля за осуществлением согласованных стандартов и рекомендаций на уровне Организации Объединенных Наций, изложенных в Динарской декларации об инициативе, касающейся стандартов в киберпространстве[7].

В рамках Группы двадцати Франция работает над тем, чтобы в соответствии с Парижским призывом в работе Группы учитывались основополагающие вопросы конкуренции в цифровой экономике, новые режимы регулирования и управления и вопросы цифровой безопасности.

В качестве активного участника неофициальной рабочей группы Организации по безопасности и сотрудничеству в Европе (ОБСЕ) по кибербезопасности Франция продолжает содействовать осуществлению 16 мер укрепления доверия, разработанных ОБСЕ в целях обеспечения кибербезопасности. В частности, она играет ведущую роль в реализации мер укрепления доверия в области обеспечения безопасности объектов критически важной инфраструктуры.

В целях усиления борьбы с распространением вредоносных методов и программных средств Франция поддержала включение программного обеспечения для несанкционированного доступа в список предметов двойного назначения Вассенаарских договоренностей по экспортному контролю за обычными вооружениями, товарами и технологиями двойного назначения. Франция уверена в том, что такого рода работу по регулированию следует продолжить и включить определенные киберпрограммы, в зависимости от серьезности их последствий, в перечень средств военного назначения.

Франция считает, что многие вопросы, связанные с кибербезопасностью, заслуживают рассмотрения в рамках многостороннего подхода, что позволит учесть конкретные роли и обязанности негосударственных субъектов. В этой связи Франция поддерживает деятельность Глобальной комиссии по стабильности в киберпространстве. Цель этой комиссии заключается в разработке

[6] URL: www.diplomatie.gouv.fr/IMG/pdf/texte_appel_de_paris_-_fr_cle0d3c69.pdf.

[7] URL: www.diplomatie.gouv.fr/IMG/pdf/g7_-_declaration_de_dinard_sur_l_initative_pour_des_normes_dans_le_cyberespace_cle8a8313.pdf.

предложений в отношении нормативных и директивных мер, направленных на укрепление международной безопасности и стабильности и на регулирование ответственного поведения государств в киберпространстве.

3. Соответствующие международные концепции укрепления глобальной кибербезопасности

a) Концепции поддержания международного мира и безопасности

Для обеспечения открытого, безопасного, стабильного, доступного и мирного киберпространства Франция вновь подтверждает свою приверженность применению норм международного права, включая все положения Устава Организации Объединенных Наций, международного гуманитарного права и международных стандартов в области прав человека, к вопросам использования государствами информационно-коммуникационных технологий.

Международное публичное право

В соответствии с заключением Группы правительственных экспертов Организации Объединенных Наций по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, изложенным в опубликованном в 2013 году докладе Группы, поведение государств в киберпространстве регулируется принципами и нормами международного права. Хотя киберпространство имеет свои особенности (анонимность, роль частных субъектов), международное право, тем не менее, обеспечивает необходимые средства для ответственного регулирования поведения государств в этой среде. В этом отношении невозможность определить местоположение не может являться непреодолимым препятствием для применения действующего международного права.

Принцип суверенитета применяется и к киберпространству. В этой связи Франция подтверждает, что она осуществляет свой суверенитет в отношении информационных систем, людей и деятельности в киберпространстве на своей территории в рамках своих обязательств по международному праву. Несанкционированное проникновение в французские системы или оказание воздействия на французской территории в результате использования киберсредств государственным учреждением или негосударственным субъектом, действующим по указанию или под контролем какого-либо государства, может являться нарушением суверенитета.

Диапазон мер, которые государства могут принимать в ответ на компьютерные атаки, зависит от тяжести нападения. Чем серьезнее будет кибератака, тем шире будет этот диапазон. Кибероперация может рассматриваться как применение силы, запрещенное в соответствии с пунктом 4 статьи 2 Устава Организации Объединенных Наций. Подпадание под определение применения силы связано не с тем, какие кибернетические средства были использованы, а с тем, к каким последствиям привела кибероперация. Если они аналогичны последствиям, возникающим в результате применения обычных вооружений, кибероперация может представлять собой применение силы. Франция считает, что серьезная компьютерная атака, совершенная государством или негосударственными субъектами, действующими под контролем государства или по его указанию, достигающая по своим масштабам или последствиям достаточно серьезного порога (например, значительная гибель людей, значительный физический ущерб или отказ критически важной инфраструктуры со значительными последствиями) и приписываемая государству, может считаться «вооруженным нападением» по смыслу статьи 51 Устава и тем самым являться основанием для осуществления права на законную самооборону. Такая самооборона может

осуществляться обычными или кибернетическими средствами при условии соблюдения принципов необходимости и соразмерности. Квалификация компьютерной атаки как вооруженного нападения по смыслу статьи 51 Устава требует принятия отдельного политического решения по каждому конкретному случаю с учетом критериев, установленных международным правом.

Франция считает, что на данном этапе разработка нового международного юридически обязательного документа, конкретно касающегося вопросов кибербезопасности, не требуется. В киберпространстве, как и в других областях, применяется и должно соблюдаться действующее международное право.

Международное гуманитарное право

Франция поддерживает применимость норм международного гуманитарного права к кибероперациям, проводимым в контексте вооруженных конфликтов и в связи с ними.

В настоящее время наступательные действия в области информационной безопасности проводятся параллельно с обычными военными операциями. Нельзя априорно исключить вероятность возникновения вооруженного конфликта, состоящего исключительно из деятельности в цифровой области, но такая вероятность будет зависеть от того, приведут ли кибероперации к такому уровню насилия, при котором их можно рассматривать в качестве международного или немеждународного вооруженного конфликта.

Несмотря на их дематериализованный характер, эти операции по-прежнему регулируются географическим охватом международного гуманитарного права, то есть их последствия ограничиваются территорией государств — сторон международного вооруженного конфликта или территорией, на которой ведутся военные действия в контексте немеждународного вооруженного конфликта.

Наступательные действия французских вооруженных сил в области информационной безопасности осуществляются в соответствии с принципами международного гуманитарного права, в частности с принципами, изложенными ниже.

- **Принцип проведения различия между гражданскими и военными объектами**. В соответствии с этим принципом, кибератаки, которые не направлены на конкретные военные объекты или которые осуществляются с помощью кибероружия, которое не может быть использовано против конкретного военного объекта, запрещены. В этой связи некоторые данные о контенте, хотя и неосязаемые по своему характеру, могут представлять собой гражданскую собственность, охраняемую в соответствии с международным гуманитарным правом.

- **Принцип гуманности**. Операции не должны также быть направлены против гражданского населения как такового или гражданских лиц, за исключением тех случаев, когда они принимают прямое участие в военных действиях, в течение такого участия. В контексте вооруженного конфликта любой киберкомбатант-военнослужащий вооруженных сил, любой член организованной вооруженной группы, совершающий кибератаки на противника или любое гражданское лицо, непосредственно участвующее в военных действиях с помощью киберсредств, может подвергнуться нападению с использованием обычных или кибернетических средств.

- **Принцип соразмерности**. При проведении операций следует постоянно проявлять осторожность и обеспечивать защиту гражданского населения и гражданского имущества от последствий боевых действий.

Сопутствующий ущерб не может быть больше ожидаемого непосредственного и конкретного военного преимущества. Соблюдение принципа соразмерности в киберпространстве требует учета всех прогнозируемых последствий применения оружия, будь то прямое (повреждение целевой системы, прерывание обслуживания или иное) или косвенное (воздействие на инфраструктуру, контролируемую атакуемой системой, а также на лиц, пострадавших от сбоя или разрушения систем, изменения и порчи данных), при условии, что они в достаточной степени непосредственно связаны с атакой. Этот принцип также запрещает применение кибероружия, которое не поддается контролю (особенно во времени и пространстве), а значит может нанести непоправимый ущерб гражданской инфраструктуре, системам или данным.

Эти элементы, в частности, упоминаются в публичной части французской военной концепции наступательных действий в области информационной безопасности, представленной в начале 2019 года.

Права человека

Франция считает, что права, которыми люди пользуются в обычной жизни, должны защищаться в том числе и при пользовании интернетом и что международное право прав человека применимо и к киберпространству. Эти ценности подрываются распространением в интернете незаконного контента (террористического, ненавистнического, антисемитского). Франция считает, что особенно важно привлекать специалистов по цифровым технологиям из частного сектора к борьбе с незаконным контентом и разъяснять их роль и обязанности на международном уровне в целях борьбы с таким незаконным контентом и обеспечения защиты прав человека и основных свобод в интернете.

Принцип должной осмотрительности

Франция считает крайне важным достижение на международном уровне общего понимания в отношении обязательств государства, чья инфраструктура используется не по назначению в ущерб интересам другого государства. Это необходимо для того, чтобы уточнить применение в кибернетической области принципа должной осмотрительности, который предусматривает, что каждое государство обязано не давать осознанного разрешения на использование своей территории для совершения действий, нарушающих права других государств[8]. В этой связи государства не должны заведомо позволять использовать свою территорию для совершения международно-противоправных деяний с использованием киберсредств и не должны использовать негосударственных посредников (доверенных лиц) для совершения нарушений международного права. Более глубокое понимание применения этого принципа к кибервопросам способствовало бы укреплению сотрудничества между государствами в целях защиты некоторых важнейших объектов инфраструктуры и предотвращения крупных кибератак, проходящих через третьи страны.

b) Концепция укрепления сотрудничества и доверия между государствами

Нормы поведения

Несколько раундов переговоров, проведенных в рамках Группы правительственных экспертов по кибербезопасности, позволили добиться значительного прогресса в области международного регулирования киберпространства. В

[8] *Дело о проливе Корфу*, судебное решение от 9 апреля 1949 года: Доклады Международного уголовного суда, 1949 год, стр. 4.

частности, в докладе за 2015 год описываются 11 стандартов ответственного поведения государств в киберпространстве. Франция считает, что каждое государство обязано соблюдать эти стандарты и разрабатывать механизмы их осуществления. В будущем можно было бы также разработать другие стандарты, применимые к поведению государств или других субъектов в киберпространстве.

Меры укрепления доверия

Необходимо продолжать работу в рамках различных региональных форумов и организаций по разработке конкретных мер укрепления доверия по вопросам кибербезопасности. Франция будет и впредь поощрять своих партнеров к принятию межведомственных процедур, которые могут быть использованы для обеспечения эффективной связи между государствами во время кризиса. Разработка таких процедур и механизмов, основанных на транспарентности и информировании, имеет важнейшее значение для предотвращения конфликтов в киберпространстве.

Развитие потенциала

Франция поддерживает задачу развития международного потенциала в области кибербезопасности. Такие усилия вносят весьма непосредственный вклад в укрепление всеобщей безопасности и стабильности киберпространства. Франция намерена в полной мере участвовать в этих усилиях путем принятия мер по наращиванию потенциала на двустороннем, региональном или многостороннем уровнях.

c) Роль и ответственность негосударственных субъектов

Подход, предусматривающий участие многих заинтересованных сторон

В Парижском призыве Франция подчеркнула необходимость укрепления многостороннего подхода. Франция считает, что гражданское общество, научные круги, частный сектор и техническое сообщество обладают навыками и ресурсами, необходимыми для определения ряда аспектов соответствующей политики в области кибербезопасности.

Ответственность частных субъектов за обеспечение безопасности при разработке и обслуживании цифровых продуктов

Появление цифровой области в качестве нового средства и пространства для конфронтации привело к тому, что на частный сектор, включая ряд системных субъектов, была возложена важнейшая роль и совершенно новая обязанность в деле поддержания международного мира и безопасности. Таким образом, в Парижском обращении Франция признает ответственность основных субъектов частного сектора за укрепление доверия, безопасности и стабильности в киберпространстве и поощряет инициативы, направленные на повышение безопасности цифровых процессов, продуктов и услуг.

Франция считает важным установить на международном уровне принцип ответственности системных частных субъектов за обеспечение безопасности при разработке, интеграции, внедрении и обслуживании их цифровых продуктов, процессов и услуг на протяжении всего их жизненного цикла и на всех этапах производственно-сбытовой цепочки.

Ответственность цифровых платформ в борьбе с терроризмом

Франция также принимает меры к тому, чтобы частные субъекты, действующие в цифровой области, несли ответственность за борьбу с неправомерным

использованием своих услуг в террористических целях. В частности, она поднимает этот вопрос в Группе семи и Европейском союзе, где активно поддерживает принятие проекта европейского постановления, призванного определить основу деятельности интернет-провайдеров в борьбе с террористическим контентом в интернете. Этот текст требует изъятия террористического контента в течение одного часа по просьбе одного из государств-членов, принятия решительных мер в отношении платформ, на которых размещается контент террористического характера, обязательства назначить контактное лицо для круглосуточной работы с уведомлениями и просьбами об изъятии, а также введения санкций в случае систематического отказа от сотрудничества.

Предотвращение атак со стороны частных субъектов

Франция считает, что государства должны сохранять монополию на законное физическое насилие во всех областях, в том числе и в киберпространстве. В этом смысле она поддерживает запрещение негосударственным субъектам, включая частный сектор, предпринимать наступательные действия в киберпространстве от своего имени или от имени других негосударственных субъектов. Такая практика, основанная на принципе частной самообороны («ответный взлом»), потенциально дестабилизирует ситуацию из-за ее негативных последствий для третьей стороны и может подпитывать возможную эскалацию отношений между государствами. В этой связи Франция считает, что необходимо добиться определения границ пространства для маневрирования, имеющегося у частных субъектов в вопросе реагирования на инциденты.

4. Меры, которые могли бы быть приняты международным сообществом для укрепления информационной безопасности на глобальном уровне

Перед лицом новых угроз, возникших в результате цифровой революции, Франция считает, что сотрудничество и право необходимы для того, чтобы киберпространство не превратилось в зону постоянного конфликта. Государства обязаны соблюдать международное право в цифровом пространстве, так же как и в других областях. Кроме того, в последние годы появился нормативный корпус, определяющий ответственное поведение государств в киберпространстве, который все еще нуждается в доработке. Франция считает, что для укрепления кибербезопасности на международном уровне можно было бы принять следующие меры:

- **углубить успехи, достигнутые на предыдущих совещаниях Группы правительственных экспертов**. Было бы полезно более подробно определить, каким образом стандарты и рекомендации, принятые на основе консенсуса в ходе предыдущих раундов переговоров, могут быть реализованы, не пересматривая при этом сами стандарты и рекомендации, и добиться более глубокого понимания имеющейся на международном уровне передовой практики в этой области;

- **взять Парижский призыв к укреплению доверия и безопасности в киберпространстве за основу дальнейших дискуссий по вопросам кибербезопасности в Организации Объединенных Наций**. На сегодняшний день эта декларация объединила более трети государств — членов Организации, а также несколько сотен значимых негосударственных субъектов вокруг общей концепции принципов, которые должны лежать в основе поведения различных участников киберпространства;

- **обеспечить универсализацию Конвенции о киберпреступности**. Этот документ, принятый в ноябре 2001 года в целях укрепления международного сотрудничества в этой области, на сегодняшний день ратифицирован

63 государствами и оказал влияние на национальное законодательство более чем двух третей государств — членов Организации Объединенных Наций;

- **содействовать повышению транспарентности между государствами**. Это в первую очередь касается их стратегий кибербезопасности, концепций предупреждения и ликвидации чрезвычайных ситуаций в области кибербезопасности и реагирования на кибератаки, а также толкования применимости международного права к киберпространству;

- **реализовать на соответствующем региональном или международном уровне уже существующие наработки, касающиеся мер укрепления доверия и учитывающие особенности киберзадач**;

- **укрепить инициативы и механизмы, позволяющие организовать обмен передовым опытом и наращивание потенциала**. Такие механизмы должны быть направлены на обеспечение всех государств эффективным механизмом кибербезопасности, в том числе посредством:

  – осуществления стратегии кибербезопасности;

  – определения законодательной базы для содействия кибербезопасности и борьбе с киберпреступностью;

  – создания группы реагирования на инциденты информационной безопасности;

  – определение процедур сотрудничества с частным сектором, включая крупные цифровые компании;

  – создание рамочной программы защиты ключевых систем инфраструктуры в киберпространстве;

- **признать на международном уровне принцип ответственности в отношении безопасности со стороны системных частных субъектов**. Эта ответственность распространяется на разработку, интеграцию, внедрение и обслуживание цифровых продуктов, процессов и услуг на протяжении всего их жизненного цикла и по всей цепочке поставок.

Греция

[Подлинный текст на английском языке]
[15 мая 2019 года]

В декабре 2018 года Генеральная Ассамблея приняла резолюцию о поощрении ответственного поведения государств в киберпространстве в контексте международной безопасности. В этой резолюции содержится просьба к Генеральному секретарю запросить мнения и оценки государств-членов по следующим вопросам: a) усилия, предпринимаемые на национальном уровне для укрепления информационной безопасности и содействия международному сотрудничеству в этой области; и b) содержание концепций, упомянутых в докладах Группы правительственных экспертов.

Греция поддерживает единодушное мнение Группы правительственных экспертов о том, что нормы международного права, и в частности Устав Организации Объединенных Наций, применимы и в киберпространстве и имеют решающее значение для поддержания мира и стабильности и содействия созданию открытой, безопасной, мирной и доступной информационно-коммуникационной среды. Греция также выступает за то, чтобы продолжить обсуждение норм

ответственного поведения государств, мер укрепления доверия и норм международного права в рамках Первого комитета Организации Объединенных Наций и создать новую Группу правительственных экспертов.

Мы признаем, что ввиду взаимосвязанного и сложного характера киберпространства от правительств, частного сектора, гражданского общества, технического сообщества, пользователей и научных кругов требуются совместные усилия для решения стоящих перед ними проблем, и призываем все заинтересованные стороны признать и взять на себя конкретные обязательства по поддержанию открытого, свободного, безопасного и стабильного киберпространства.

Мы признаем также роль Организации Объединенных Наций в дальнейшей разработке норм ответственного поведения государств в киберпространстве и напоминаем, что по итогам обсуждений в Группе правительственных экспертов был выработан согласованный комплекс норм и рекомендаций, которые неоднократно одобрялись Генеральной Ассамблеей и которые государствам следует принять за основу для ответственного поведения в киберпространстве.

Как член международных организаций, таких как Организация Объединенных Наций, Европейский союз, Организация Североатлантического договора и Организация по безопасности и сотрудничеству в Европе, мы стремимся установить универсальные правила и принципы ответственного поведения государств при использовании киберпространства, сотрудничать, обмениваться опытом и передовой практикой и совместно разрабатывать надлежащие средства для устранения угроз и вызовов, связанных с кибербезопасностью. Наша страна в максимально возможной степени содействует формулированию и исполнению соответствующих решений, принимаемых в рамках международных организаций, в целях расширения сотрудничества, повышения транспарентности и снижения риска возникновения конфликтов.

Признавая, что киберпреступность является глобальной проблемой, Греция подписала и ратифицировала Конвенцию Совета Европы о киберпреступности, известную также как Будапештский договор. Этот договор обеспечивает важную основу как для принятия в нашей стране национальных законов, так и для международного сотрудничества в борьбе с киберпреступностью. Будапештский договор был ратифицирован Законом 4411/2016. Кроме того, как член Организации по безопасности и сотрудничеству в Европе наша страна также подписала Соглашение о мерах укрепления доверия, цель которого — наладить между государствами-членами сотрудничество по вопросам кибербезопасности, обеспечить транспарентность и стабильность и снизить риск конфронтации в киберпространстве.

Выполняя свои обязательства как член Европейского союза, Греция включила в свое национальное законодательство Директиву 1148 о безопасности сетей и информационных систем (Директива NIS — по первым буквам ее названия на английском языке), предусматривающую меры по обеспечению высокого общего уровня безопасности на всей территории Союза, и занимается внедрением мер обеспечения кибербезопасности, разработкой национальной стратегии в этой сфере и укреплением сотрудничества с государствами-членами. Результатом стало усиление защиты всех важнейших объектов инфраструктуры в нашей стране при соблюдении принципов открытого общества, конституционных свобод и индивидуальных прав. Общая ответственность за реализацию национальной стратегии кибербезопасности возложена на Национальное управление кибербезопасности, которое действует под эгидой министерства цифрового управления.

Основные цели нашей национальной стратегии кибербезопасности перечислены ниже:

- развитие и укрепление защищенного и устойчивого киберпространства на основе национальных, европейских и международных стандартов и практики;
- постоянное совершенствование наших возможностей по защите от кибератак с упором на защиту важнейших объектов инфраструктуры;
- формирование прочной культуры общественной и частной безопасности с использованием потенциала как академического сообщества, так и государственных и частных структур;
- повышение уровня оценки, анализа и предотвращения угроз с целью обеспечить безопасность информационных систем и инфраструктур;
- создание эффективной основы для координации и сотрудничества между государственными и частными заинтересованными сторонами;
- активное участие нашей страны в международных инициативах и мероприятиях международных организаций в области кибербезопасности;
- повышение осведомленности всех заинтересованных сторон из числа общественных групп и информирование пользователей о безопасном использовании киберпространства;
- постоянная адаптация работы национальных учреждений к новым технологическим требованиям и европейским директивам;
- содействие инновациям, исследованиям и разработкам по вопросам безопасности.

Япония

[Подлинный текст на английском языке]
[14 мая 2019 года]

1. Общая оценка проблем информационной безопасности

Все большее распространение в обществе получают знания, технологии и услуги, связанные с использованием киберпространства, такие как искусственный интеллект, интернет вещей, финансовые технологии (финтех), большие данные и стандарт мобильной связи пятого поколения (5G), способствуя инновациям, которые кардинально меняют существующие структуры в нашей социально-экономической деятельности и повседневной жизни людей, в результате чего происходит сближение виртуального и реального пространства. Для того чтобы пользоваться преимуществами таких знаний, технологий и услуг, крайне необходимо контролировать присущие им скрытые риски. В тех случаях, когда контролировать эти риски нельзя, существует вероятность быстрого роста угроз кибербезопасности.

Преимущества киберпространства

В мире растет число пользователей Интернета, и стремительными темпами идет распространение самого Интернета. Кроме того, значительно увеличилось количество владельцев личных смартфонов и растут показатели использования Интернета. Растет и число пользователей социальных сетей, которые теперь могут с легкостью общаться друг с другом в киберпространстве. Расширение масштабов пользования обществом виртуальными услугами способствовало не

только свободному распространению информации, но и формированию разнообразных сообществ и обмену информацией. Прогресс наблюдается и в области финансовой деятельности, включая интернет-торговлю, биржевой торг и банковское обслуживание через Интернет; так, регулярно появляются новые услуги в области финансовых технологий и экономики совместного потребления, продвигая вперед инновационную деятельность. Был также достигнут прогресс в использовании информационно-коммуникационных технологий в медицине и сестринском деле, в сферах социального обеспечения и образования и в других областях, связанных с такими социальными вопросами, как сокращение численности населения трудоспособного возраста и старение местных общин.

Растущие угрозы в киберпространстве

Хотя искусственный интеллект, интернет вещей и другие технологии и услуги потенциально могут принести людям много пользы, всегда существует скрытый риск того, что поставщики этих технологий и услуг утратят способность их контролировать, результатом чего могут стать неизмеримые экономические и социальные потери или ущерб. По мере сближения виртуального и реального пространства вероятность такого сценария возрастает в геометрической прогрессии. Кроме того, киберпространство представляет собой не ограниченное пространством или временем место, в котором любой человек, включая злоумышленников, может без труда злоупотреблять новыми информационно-коммуникационными технологиями и использовать их не по назначению. Сам характер цифровых технологий позволяет злоумышленникам легко копировать и распространять конфиденциальные данные и информацию, запускать вредоносные программы, гибко внедрять и свободно использовать новые технологии, такие как искусственный интеллект и блокчейн. Поэтому нападающие имеют асимметричное преимущество перед защитниками, которое, как ожидается, будет увеличиваться, особенно в тех случаях, когда построение защитников зависит от существующих стратегий и технологических систем. В этих условиях совершаются атаки на интернет вещей, финансовые технологии, включая криптовалюты, важнейшие объекты инфраструктуры и цепочки поставок, что, помимо обычного нарушения безопасности данных, приводит к прямым финансовым потерям и сбоям в работе предприятий и оказании услуг, создавая угрозу устойчивому развитию социально- экономической деятельности и безопасности жизни людей. Кроме того, следует отметить массовые инциденты, которые, как предполагается, финансировались государствами. Существует также опасение, что доверие к информационной инфраструктуре может быть подорвано, если киберпространство будет контролироваться и управляться правительствами некоторых стран с позиции превосходства. Ожидается, что по мере сближения виртуального и реального пространства будет увеличиваться риск возможных попыток воспользоваться уязвимостями интернета вещей, цепочек поставок и открытых инноваций и нежелательного поведения в этих системах. Это может серьезно сказаться не только на государственных органах и операторах критически важных объектов инфраструктуры, но и на других предприятиях и даже частных лицах.

Принципиальная позиция по вопросам киберпространства

Для того чтобы и далее предотвращать действия злоумышленников, обеспечивать безопасность людей и гарантировать их права, Япония имеет в своем арсенале политические, экономические, технологические, правовые, дипломатические и другие практические и эффективные средства. При разработке и внедрении мер обеспечения кибербезопасности Япония придерживается следующих пяти принципов: i) обеспечение свободного распространения

информации; ii) верховенство права; iii) открытость; iv) автономность; и v) сотрудничество между различными заинтересованными сторонами.

i) Обеспечение свободного распространения информации

Для устойчивого развития киберпространства как площадки для творчества и инноваций крайне важно создавать и поддерживать такие условия, в которых передаваемая информация доходила бы до предполагаемого получателя, не подвергаясь несправедливой цензуре или незаконным изменениям. Необходимо также соблюдать принцип конфиденциальности. Одним из основных условий свободного распространения информации в киберпространстве является требование руководствоваться принципами морали и здравым смыслом, чтобы не ущемлять права и интересы других.

ii) Верховенство права

По мере сближения виртуального и реального пространства принципы верховенства права должны соблюдаться в киберпространстве таким же образом, как и в реальности. В киберпространстве применяются различные национальные правила и нормы, включая внутренние законы и положения. Помимо этого, там применяются и нормы международного права. Применение существующих норм международного права и разработка новых норм по-прежнему имеют огромное значение для устойчивого развития киберпространства как безопасной и надежной площадки.

iii) Открытость

Для того чтобы киберпространство развивалось как площадка для формирования новых ценностей, оно должно быть открытым для всех участников и не ограничивать распространение различных идей и знаний. Япония полагает, что в киберпространстве не должна доминировать какая-то одна небольшая группа лиц.

iv) Автономность

Киберпространство развивается благодаря автономным инициативам многих заинтересованных сторон. Неуместно и невозможно, чтобы какое-либо государство полностью брало на себя всю ответственность за поддержание порядка, если мы хотим, чтобы киберпространство устойчиво развивалось как площадка, на которой сосуществуют порядок и творчество. Единственный способ поддерживать порядок, сдерживать злоумышленников и бороться с их поведением — это обеспечить автономное функционирование различных социальных систем. Япония выступает именно за такой подход.

v) Сотрудничество между различными заинтересованными сторонами

Киберпространство — это многомерный мир, создаваемый в результате деятельности многих заинтересованных сторон, в том числе государства, местных органов власти, операторов важнейших объектов инфраструктуры, связанных с киберпространством и других предприятий, образовательных и научно-исследовательских учреждений и отдельных лиц. Для того чтобы киберпространство развивалось на устойчивой основе, все участники должны добросовестно выполнять свои соответствующие функции и обязанности. Для этого, помимо индивидуальных усилий, требуются координация и сотрудничество. Ведущую роль в содействии такой координации и сотрудничеству играют государства, которые поощряют меры, способствующие выполнению таких функций.

2. Усилия, предпринимаемые на национальном уровне для укрепления информационной безопасности и содействия международному сотрудничеству в этой области

Усилия, предпринимаемые на национальном уровне для укрепления информационной безопасности

В Японии была подготовлена правовая основа для использования данных, включая Основной закон о более эффективном использовании данных государственного и частного секторов, Закон о защите личной информации с внесенными в него поправками и другие. Правительство также проводит политику формирования антропоцентричного общества, в котором было бы возможным как экономическое развитие, так и решение социальных проблем на основе высокой степени интеграции виртуального и реального пространства. В этих условиях в настоящее время в киберпространстве накапливаются и анализируются огромные объемы данных, получаемых с помощью датчиков и устройств в реальном пространстве. Кроме того, в реальном пространстве можно наблюдать, как в целом ряде сфер периодически предлагаются новые продукты и услуги, создающие добавленную стоимость за счет использования данных. Киберпространство и реальное пространство больше нельзя считать отдельными, независимыми площадками, поскольку они существуют во взаимосвязи друг с другом. Поэтому эти два пространства следует рассматривать как единое, непрерывно развивающееся целое.

Сближение виртуального и реального пространства значительно расширяет возможности для обеспечения благополучия в обществе. В то же время у злоумышленников оказывается больше возможностей злоупотреблять киберпространством. Ожидается, что риск экономических и социальных потерь или ущерба в реальном пространстве будет возрастать в геометрической прогрессии. В этих условиях необходимо обеспечить безопасность киберпространства, которое служит основой экономического общества, и в то же время необходимо сделать так, чтобы оно развивалось автономно и непрерывно, что позволит достичь устойчивого прогресса и гарантировать благосостояние общества.

В последнее время определенные государства склоняются к тому, чтобы в ответ на киберугрозы реагировать ужесточением контроля над киберпространством. Однако ужесточение государственного контроля над киберпространством препятствует его автономному, устойчивому развитию. Таким образом, необходимо уважать сегодняшнее киберпространство, развивающееся на основе автономных инициатив всех заинтересованных сторон, и обеспечивать кибербезопасность в рамках совместных усилий, предпринимаемых с этими заинтересованными сторонами. Исходя из этого понимания, памятуя о планах на 2020 год и последующий период и принимая во внимание проведение таких международных мероприятий, как XXXII Олимпийские игры и Паралимпийские игры 2020 года в Токио (далее именуемые «Игры-2020 в Токио»), Япония приложит все возможные усилия к тому, чтобы пояснить основные принципы кибербезопасности, выявить новые вопросы, требующие решения, и оперативно принять соответствующие меры.

Усилия, предпринимаемые на национальном уровне для содействия международному сотрудничеству

Поскольку последствия инцидентов в киберпространстве могут легко распространяться за пределы национальных границ, всегда существует вероятность того, что от них может пострадать и Япония. Япония будет сотрудничать и взаимодействовать с правительствами и частным сектором во всем мире в целях обеспечения безопасности киберпространства и работать как на благо мира и

стабильности международного сообщества, так и на благо своей национальной безопасности. С этой целью правительство нашей страны будет активно участвовать в различных международных обсуждениях и содействовать обмену информацией и выработке общего понимания по вопросам, связанным с киберпространством. Кроме того, правительство нашей страны будет также делиться опытом с зарубежными странами, налаживать конкретное сотрудничество и взаимодействие и принимать соответствующие меры.

Что касается обмена опытом и координации политики, то правительство, действуя в рамках двусторонних диалогов и международных конференций по кибербезопасности, будет содействовать обмену информацией о политике, стратегиях и системах реагирования в области кибербезопасности, используя эти знания при планировании политики Японии в области кибербезопасности. Мы также будем укреплять наше сотрудничество и взаимодействие в области политики кибербезопасности со стратегическими партнерами, которые разделяют наши основные принципы кибербезопасности.

Что касается международного сотрудничества в деле реагирования на инциденты, то наше правительство будет обмениваться информацией о кибератаках и угрозах и укреплять сотрудничество между группами по реагированию на чрезвычайные ситуации в компьютерной сфере, с тем чтобы обеспечить принятие скоординированных мер реагирования в случае возникновения инцидентов. Правительство будет также работать над укреплением потенциала скоординированного реагирования путем организации совместной подготовки и участия в международных практикумах по кибербезопасности и совместных учебных мероприятиях. Кроме того, в случае возникновения инцидентов правительство будет принимать надлежащие меры реагирования на основе соответствующего международного сотрудничества.

С учетом дипломатических аспектов международного сотрудничества в области кибербезопасности мы взяли на себя обязательства в трех основных сферах: верховенство права, принятие мер укрепления доверия и наращивание потенциала в киберпространстве.

- Поощрение верховенства права имеет большое значение для международного мира и стабильности и национальной безопасности Японии. Позиция Японии заключается в том, что действующее международное право, включая Устав Организации Объединенных Наций, также применимо к киберпространству, и Япония будет активно содействовать обсуждению вопросов индивидуального и конкретного применения действующего международного права и разработки и универсализации норм. Что касается мер по борьбе с киберпреступностью, то Национальное полицейское управление в сотрудничестве с другими соответствующими министерствами и ведомствами будет работать над дальнейшим укреплением международного партнерства, налаживая международное сотрудничество при проведении расследований и обмен информацией с международными организациями, правоохранительными органами и органами информационной безопасности в иностранных государствах и задействуя такие механизмы, как Конвенция о киберпреступности, договоры о взаимной правовой помощи и Международная организация уголовной полиции (Интерпол).

- Япония будет работать над укреплением доверия между государствами, с тем чтобы предотвратить возникновение непредвиденных обстоятельств и ухудшение ситуации, вызванное кибератаками. Из-за анонимного и секретного характера кибератак существует риск того, что кибератаки могут непреднамеренно усилить напряженность в отношениях между государствами и привести к ухудшению ситуации. Для предотвращения таких

случайных и ненужных конфронтаций важно, чтобы в мирное время налаживались международные каналы связи в процессе подготовки к инцидентам, последствия которых выходят за пределы национальных границ. Необходимо также повышать транспарентность и укреплять доверие между государствами посредством активного обмена информацией и диалога по вопросам политики в рамках двусторонних и многосторонних консультаций. Наше правительство будет также сотрудничать с другими государствами в целях рассмотрения вопроса о создании механизма координации вопросов, касающихся киберпространства. В этой связи Япония активно содействует принятию мер укрепления доверия, в том числе путем созыва межсессионного совещания по вопросам кибербезопасности Ассоциации государств Юго-Восточной Азии (АСЕАН), на котором она выступила в роли сопредседателя, и неизменно оказывает помощь в наращивании потенциала главным образом странам в Азиатско-Тихоокеанском регионе.

- Что касается наращивания потенциала, то ввиду усиления взаимозависимости между странами Япония не в состоянии обеспечить мир и стабильность в одиночку. Огромное значение для обеспечения национальной безопасности Японии имеет глобальная координация в целях сокращения и устранения факторов уязвимости в области кибербезопасности. С этой точки зрения содействие наращиванию потенциала в других государствах обеспечивает стабильность жизни и деятельности в этих странах японских граждан и компаний, которые пользуются ключевыми объектами инфраструктуры и зависят от грамотного использования киберпространства. В то же время меры по наращиванию потенциала также напрямую связаны с обеспечением безопасности всего киберпространства и способствуют улучшению обстановки в области безопасности во всем мире, включая Японию. Кроме того, что касается киберпреступности, то Япония является одним из немногих неевропейских участников Конвенции о киберпреступности и всячески содействует ее осуществлению как важной правовой основы для борьбы с киберпреступностью, оказывая помощь странам Азиатского региона в наращивании потенциала.

3. Важные международные концепции по укреплению безопасности глобальных информационных и телекоммуникационных систем

Япония поддерживает выводы, к которым на основе консенсуса пришли предыдущие группы правительственных экспертов, о том, что действующее международное право применяется в киберпространстве. Мы считаем, что ключом к формированию ответственного поведения государств в киберпространстве является обсуждение таких вопросов, как разработка принципов нормативного поведения, принятие мер укрепления доверия и наращивание потенциала. В частности, Япония признает, что соблюдение добровольных и необязывающих норм ответственного поведения государств в киберпространстве, о которых говорится в докладе Группы правительственных экспертов по достижениям в области информатизации и телекоммуникаций в контексте международной безопасности за 2015 год, должно стать основой для обеспечения международной стабильности и предсказуемости и для проведения в будущем обсуждений по этому вопросу. В этой связи мы считаем, что любые попытки заключить новые всеобъемлющие договоры или аналогичные документы в данный момент не приведут к реальному усилению кибербезопасности.

4. Возможные меры, которые могли бы быть приняты международным сообществом для укрепления информационной безопасности на глобальном уровне

Япония как ответственное государство, поддерживающее координацию международного сообщества с соответствующими региональными структурами на основе действующего международного права и все концепции, определенные Группой правительственных экспертов, полагает, что выработка общего понимания добровольных и необязывающих норм ответственного поведения государств и их применение будут способствовать укреплению международной безопасности.

5. Содержание концепций, упомянутых в докладах Группы правительственных экспертов

По мнению Японии, всем государствам было бы важно и полезно принять во внимание перечисленные ниже концепции, которые были определены Группой правительственных экспертов.

Влияние злонамеренных кибератак на международное сообщество

Для того чтобы гибко интегрировать стремительно развивающиеся информационно-коммуникационные технологии в нашу жизнь и предотвратить ущерб от злонамеренных кибератак, мы должны признать важность прогнозирования существующих и потенциальных угроз в киберпространстве и их влияния на международное сообщество.

Соблюдение добровольных и необязывающих норм ответственного поведения государства

Для того чтобы свести к минимуму последствия злонамеренных кибератак и остановить злоумышленников, мы должны не забывать о важности консенсусного доклада Группы правительственных экспертов, включая упоминаемые в нем добровольные и необязывающие нормы ответственного поведения государств. Нам следует углубить наши обсуждения в сотрудничестве с соответствующими региональными организациями, с тем чтобы обеспечить практическое и эффективное применение этих полезных усилий.

Содействие соблюдению добровольных и необязывающих норм ответственного поведения государств и сотрудничество в целях принятия соответствующих мер укрепления доверия и наращивания потенциала

Для дальнейшего укрепления усилий каждого государства по развитию и поддержанию свободного, справедливого и безопасного киберпространства в контексте международной безопасности нам следует подтвердить, что все государства твердо намерены устранять изъяны в плане безопасности в киберпространстве и предотвращать киберпреступность и другие злонамеренные действия. В этой связи членам группы следует поощрять все государства к последовательному соблюдению добровольных и необязывающих норм ответственного поведения государств, включая меры укрепления доверия и сотрудничество в целях наращивания национального потенциала по соблюдению вышеупомянутых добровольных и необязывающих норм и рекомендаций, в том числе в контексте работы следующей Группы правительственных экспертов и рабочей группы открытого состава.

Сингапур

[Подлинный текст на английском языке]
[13 мая 2019 года]

Сингапур признает, что угрозы открытому, безопасному и мирному киберпространству приобретают все более изощренный, трансграничный и асимметричный характер. Как малое государство с высокой степенью подключенности к Интернету, которое не раз становилось объектом кибератак, Сингапур решительно поддерживает идею установления в киберпространстве порядка, основанного на нормах международного права. Это позволит укрепить доверие между государствами-членами и будет способствовать социально-экономическому прогрессу. Чтобы в полной мере воспользоваться преимуществами цифровых технологий, международное сообщество должно создать защищенное, надежное и открытое киберпространство, опирающееся на применимые к нему нормы международного права, тщательно проработанные нормы ответственного поведения государств, эффективные меры укрепления доверия и скоординированные усилия по наращиванию потенциала. В совокупности эти три взаимоукрепляющих компонента позволят создать безопасное и устойчивое к внешним воздействиям киберпространство. Важно, чтобы государства продолжали свои усилия по обсуждению таких законов, правил и норм в рамках Организации Объединенных Наций — единственного универсального, всеохватного и многостороннего форума, в котором все государства, независимо от размера, имеют право голоса. Сингапур готов играть свою роль в этом процессе.

Сингапур с удовлетворением отмечает создание Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и решение созвать рабочую группу открытого состава. По мнению Сингапура, усилия Группы правительственных экспертов и рабочей группы могут и должны дополнять друг друга. Важно, чтобы основные субъекты работали сообща в духе консенсуса, взаимоуважения и взаимного доверия. Сингапур уверен в том, что обе платформы могут позитивно дополнять друг друга, и готов вносить конструктивный вклад в оба процесса.

На региональном уровне Сингапур вместе с другими государствами — членами Ассоциации государств Юго-Восточной Азии (АСЕАН) работал над первым заявлением лидеров АСЕАН о сотрудничестве в области кибербезопасности, с которым они выступили в ходе тридцать второго саммита АСЕАН в апреле 2018 года. В этом заявлении лидеры АСЕАН подтвердили необходимость установления в киберпространстве международного порядка, основанного на правилах. Они также поручили соответствующим министрам определить подходящий механизм или платформу для координации политики, дипломатии, сотрудничества, технических усилий и усилий по наращиванию потенциала в области кибербезопасности в рамках АСЕАН, а также составить конкретный перечень добровольных, практических норм поведения государств в киберпространстве, над принятием которых АСЕАН мог бы работать. В сентябре 2018 года, действуя на основании заявления лидеров, о котором говорилось выше, участники третьей Конференции на уровне министров стран — членов АСЕАН по вопросам кибербезопасности, состоявшейся в Сингапуре, договорились принципиально поддержать 11 норм, содержащихся в докладе Группы правительственных экспертов за 2015 год (A/70/174), а также сосредоточить внимание на расширении региональных возможностей по соблюдению этих норм.

Для того чтобы государства расширяли свои возможности по эффективному соблюдению правил и норм поведения, крайне важно работать над

укреплением потенциала. В Сингапуре проводится Программа АСЕАН в сфере киберпотенциала стоимостью 10 млн сингапурских долларов — модульная, многодисциплинарная и многосторонняя программа, направленная на создание в странах АСЕАН потенциала, необходимого для выработки политики и стратегий и решения технических вопросов в киберпространстве. Со времени запуска программы в 2016 году обучение по ней прошли 160 должностных лиц АСЕАН. Кроме того, Сингапур в партнерстве с Управлением по вопросам разоружения разработал программный онлайновый учебный курс, призванный углубить понимание этой темы и содействовать исполнению договоренностей, достигнутых Группой правительственных экспертов. Он также будет сотрудничать с Управлением в реализации совместной программы Организации Объединенных Наций и Сингапура, направленной на повышение осведомленности о нормах поведения в киберпространстве и стратегическом планировании киберсценариев в государствах — членах АСЕАН. В рамках расширения Программы АСЕАН в сфере киберпотенциала Сингапур в 2019 году откроет центр передового опыта АСЕАН-Сингапур в области кибербезопасности стоимостью 30 млн сингапурских долларов в целях дальнейшего укрепления политики в области кибербезопасности, разработки стратегий и наращивания технического и оперативного потенциала в странах АСЕАН. Центр будет открытым и инклюзивным, и государства — члены АСЕАН смогут использовать его для более тесного взаимодействия с международными партнерами.

На национальном уровне Сингапур добился значительных успехов в укреплении кибербезопасности своих систем и сетей по следующим трем направлениям: создание устойчивой к внешним воздействиям инфраструктуры, формирование более безопасного киберпространства и развитие динамичной экосистемы кибербезопасности.

a) *создание устойчивой к внешним воздействиям инфраструктуры.* Трансграничные киберугрозы все чаще подвергают опасности важнейшие объекты инфраструктуры разных стран. В особенности это касается наднациональной информационной инфраструктуры, в частности в финансовом, морском, телекоммуникационном и авиационном секторах, где последствия успешной кибератаки могут распространиться за пределы национальных границ и затронуть взаимосвязанные центры по всему миру. Одним из главных событий 2018 года стало принятие и введение в действие Закона о кибербезопасности, который заложил правовую основу для осуществления надзора за выполнением функций по обеспечению и поддержанию национальной кибербезопасности в Сингапуре. В этом законе особо подчеркивается, насколько важно заблаговременно обеспечить защиту ключевых объектов информационной инфраструктуры — компьютеров или компьютерных систем, обеспечивающих предоставление основных услуг, — от кибератак. Для обеспечения защиты следует обязать владельцев таких объектов инфраструктуры принять следующие меры: i) создать механизмы для выявления угроз и инцидентов в области кибербезопасности и информирования о таких инцидентах; ii) проводить регулярные оценки рисков и ревизию ключевых объектов информационной инфраструктуры; и iii) принимать участие в практикумах по кибербезопасности, проводимых национальным управлением кибербезопасности. В соответствии с этим законом, помимо усиления защиты такой инфраструктуры, национальное управление кибербезопасности уполномочено также заниматься предупреждением, расследованием угроз и инцидентов в области кибербезопасности и реагированием на них;

b) *формирование более безопасного киберпространства.* В январе 2019 года Сингапур получил статус страны, уполномоченной выдавать сертификаты в соответствии с соглашением о признании общих критериев — международным соглашением о взаимном признании сертификатов соответствия общим

критериям 30 странами. Общие критерии — это технический стандарт, используемый при оценке и сертификации средств защиты информационных технологий и широко применяемый как правительствами, так и сектором ИКТ. В настоящее время Сингапур является одной из 18 стран, получивших разрешение на выдачу сертификатов в соответствии с этим соглашением (всего государств — членов соглашения 30). В этой связи Сингапуру разрешено сертифицировать средства защиты информационных технологий на местном уровне, что способствует повышению качества средств кибербезопасности, выпускаемых малыми и средними предприятиями в Сингапуре, поскольку устанавливается их соответствие международным стандартам безопасности;

c) *развитие динамичной экосистемы кибербезопасности.* Сингапур признает, что укрепление кибербезопасности предполагает создание экосистемы кибербезопасности и поощрение инноваций в этой отрасли. В этой связи в марте 2018 года Сингапур открыл свой первый интегрированный центр предпринимательства в области кибербезопасности под названием «Инновационная экосистема кибербезопасности в Блоке 71», призванный укрепить растущую экосистему кибербезопасности Сингапура путем привлечения и развития талантов и «глубоких технологий», с тем чтобы содействовать смягчению стремительно растущих рисков в области кибербезопасности. Он также помогает создавать стартапы в сфере кибербезопасности по всему миру, реализуя целый ряд программ в поддержку предпринимателей — от генерирования идей до ускорения и расширения масштабов деятельности стартапов в сфере кибербезопасности для выхода на глобальный рынок.

Турция

[Подлинный текст на английском языке]
[10 мая 2019 года]

Информационно-коммуникационные технологии (ИКТ) прочно вошли в социальную и экономическую жизнь. Они используются в самых различных сферах, охватывающих деятельность государственного и частного секторов, важнейшие объекты инфраструктуры и отдельных людей, и получили широкое распространение в нашей стране и во всем мире. В результате ИКТ играют важную роль в достижении устойчивого роста и развития. Однако чем больше мы используем технологии, тем сильнее мы от них зависим и тем больше оказываемся подверженными рискам, которые сопряжены с их использованием. Отдельные лица, компании, критически важные объекты инфраструктуры и государства — все они сталкиваются с серьезными проблемами, вызванными киберугрозами.

С распространением технологий во всех сферах нашей жизни связано возникновение рисков нового порядка в контексте кибербезопасности. Обеспечение кибербезопасности — это не только необходимость противодействовать угрозам в высокотехнологичных областях, но и важный фактор, влияющий на благосостояние и национальную безопасность государств в силу рисков, которые отсутствие такой безопасности создает для социально-экономической жизни.

Недостатки в обеспечении безопасности ИКТ могут привести к выходу из строя критически важных систем, их эксплуатации злоумышленниками или даже к гибели людей, крупномасштабным экономическим потерям, нарушению общественного порядка или угрозам национальной безопасности.

Турция уделяет основное внимание принятию мер, необходимых для повышения национальной кибербезопасности, и реализует национальную стратегию и план действий в области кибербезопасности, рассчитанные на период 2016–2019 годов, в целях обеспечения национальной кибербезопасности, разработки и координации эффективной и устойчивой политики и претворения этой политики в жизнь. За разработку политики, стратегий и планов действий в области национальной кибербезопасности в Турции отвечает Министерство транспорта и инфраструктуры. В этом контексте были разработаны национальная стратегия и план действий в области кибербезопасности с привлечением всех соответствующих заинтересованных сторон к работе исследовательских комиссий, которую координировало Министерство транспорта и инфраструктуры.

Эти стратегия и план действий преследуют две основные цели: во-первых, признание всеми заинтересованными сторонами того, что кибербезопасность является неотъемлемой частью национальной безопасности, и, во-вторых, развитие навыков, которые позволят принимать административные и технические меры предосторожности для поддержания абсолютной безопасности всех систем и заинтересованных сторон в национальном киберпространстве.

Каждое действие, предусмотренное стратегией и планом действий, выполняется Министерством транспорта и инфраструктуры и соответствующими органами, причем прогресс по каждому из них контролируется Министерством.

С 2013 года функции группы по реагированию на чрезвычайные ситуации в компьютерной сфере Турции выполняет Управление информационно-коммуникационных технологий. Оно отвечает за все регулирующие функции, касающиеся электронных коммуникаций и почтовых услуг в Турции. Кроме того, оно уполномочено принимать необходимые меры для борьбы с кибератаками в целях обеспечения национальной кибербезопасности. Группа действует в качестве координационного центра на национальном уровне, и в ее задачу входит выявление угроз кибербезопасности страны, принятие мер по уменьшению или устранению последствий возможных кибератак и обмен информацией с определенными субъектами. Она координирует действия всех заинтересованных сторон — государственных или частных учреждений и отдельных лиц — по выявлению и устранению киберугроз. Ее основные направления в области кибербезопасности перечислены ниже:

- наращивание киберпотенциала;
- принятие технических мер;
- сбор и распространение информации об угрозах;
- защита критически важных объектов инфраструктуры.

Что касается наращивания потенциала, то к числу предпринимаемых в этом направлении действий относятся управление людскими ресурсами, подготовка кадров и проведение подготовительных мероприятий. В рамках этой деятельности мы организуем соревнования по кибербезопасности в формате «захват флага». Мы считаем, что людские ресурсы являются одним из важнейших факторов обеспечения кибербезопасности. Главные проекты по наращиванию потенциала мы реализуем в контексте национальной Группы по реагированию на чрезвычайные ситуации в компьютерной сфере. Так, мы организуем курсы обучения по вопросам кибербезопасности для институциональных групп по реагированию на чрезвычайные ситуации в компьютерной сфере из различных критически важных секторов, таких как энергетика, здравоохранение и государственные услуги. Мы также проводим практические занятия и конкурсы для

студентов и выпускников. За последние два года в наших учебных программах по кибербезопасности приняли участие более 2500 человек.

Мы также создали киберполигон с целью улучшить наши учебные программы и расширить возможности для практики. Киберполигон также используется для оценки уровня знаний и выдачи сертификатов участникам.

В рамках наших исследований по техническим мерам проводятся мероприятия, посвященные раннему обнаружению, сигнализации и оповещению. С этой целью мы разработали ряд систем обнаружения и предупреждения. Эти системы играют огромную роль в повышении уровня национальной кибербезопасности в стране за счет распознавания и обнаружения командных и контрольных центров бот-сетей и вредоносного программного обеспечения.

В рамках усилий по укреплению кибербезопасности Турция уделяет особое внимание еще одной важной области — сбору информации о киберугрозах. На этом направлении мы работаем в координации с целым рядом субъектов, в частности структурами, работающими в сфере Интернета, международными организациями, судебными органами, исследовательскими центрами и частными компаниями. Кроме того, при государственных и частных учреждениях были созданы секторальные группы по реагированию на чрезвычайные ситуации в компьютерной сфере для критически важных объектов инфраструктуры и более 1000 институциональных групп по реагированию на чрезвычайные ситуации в компьютерной сфере.

Поскольку киберпространство не имеет границ, той или иной стране трудно обеспечить кибербезопасность в одиночку. Это многосторонняя и междисциплинарная задача. Для того чтобы противостоять киберугрозам, мы работаем с пользователями, частным сектором, неправительственными организациями, научными кругами и международными партнерами. Например, турецкая Группа по реагированию на чрезвычайные ситуации в компьютерной сфере получает электронные уведомления от различных национальных групп по реагированию на чрезвычайные ситуации в компьютерной сфере и информирует соответствующие стороны, с тем чтобы те приняли необходимые меры. Она также отправляет информацию о киберугрозах и обменивается разведывательными данными с другими национальными группами по реагированию на чрезвычайные ситуации в компьютерной сфере и международными организациями.

В 2017 году при Управлении информационно-коммуникационных технологий был создан Центр безопасного Интернета, в задачу которого входит повышение осведомленности о надлежащем и безопасном использовании Интернета.

В стране действуют справочная линия и безопасный веб-сайт, где семьи могут получить консультации по вопросам эффективного пользования Интернетом. Кроме того, дети и молодые люди с ограниченным доступом к ИКТ могут воспользоваться ИКТ-услугами на борту специального грузовика «За более безопасный Интернет». Благодаря этому оснащенному средствами ИКТ грузовику люди могут непосредственно опробовать современные технологии, а дети, которые чаще пользуются Интернетом и технологиями, могут узнать о безопасном и добросовестном пользовании Интернетом.

Управление информационно-коммуникационных технологий ежегодно организует мероприятие, посвященное Дню безопасного Интернета. Главной темой 2018 года было «Создавай, подключайся и уважай других: безопасный Интернет начинается с тебя». Управление и Университет Бахчешехир объявили конкурс настольных игр, на котором молодые люди в возрасте от 12 до 18 лет должны были создать игру на заданную международную тему. Участники конкурса прислали множество проектов игр, и победители получили награды. В

ходе этого мероприятия компании «Фейсбук» и «Гугл» провели для студентов семинары по цифровым играм и более безопасному Интернету.

Кроме того, Управление подписало с Министерством социального обслуживания и семьи, Ассоциацией интернет-провайдеров и Министерством образования соглашения о мероприятиях по повышению осведомленности и подготовке инструкторов по вопросам добросовестного и безопасного использования ИКТ и Интернета. Возможность пройти эту подготовку, которая была включена в модули дистанционного обучения, была предоставлена всем преподавателям, занятым в системе Министерства образования. Благодаря этой системе дистанционного обучения к настоящему времени подготовку прошли учителя и тысячи учащихся.

В обеспечении и поддержании безопасности киберпространства решающую роль играют не только координация усилий на национальном уровне, но и международное сотрудничество, обмен информацией и укрепление доверия.

Ниже приводится информация о проводимых в Турции работе и исследованиях на предмет сферы применения мер укрепления доверия, о которых говорится в докладе Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности за 2015 год (A/70/174), и определенной в этом докладе концепции ответственного поведения государств.

На фоне широкого распространения ИКТ в качестве объекта для своих нападений в Интернете злоумышленники все чаще выбирают личные данные и информацию. В контексте основных прав и свобод человека особую обеспокоенность вызывает проблема защиты личных данных и информации.

Наряду с принципами транспарентности, подотчетности и нравственности при работе в киберпространстве все турецкие заинтересованные стороны соблюдают принцип верховенства права, основные права и свободы человека и защиты частной жизни, одновременно принимая меры к обеспечению кибербезопасности.

В этой связи 7 апреля 2016 года вступил в силу Закон № 6698 о защите персональных данных, опубликованный в официальном вестнике № 29681. Целью этого закона является защита основных прав и свобод человека, в частности права на неприкосновенность частной жизни, при обработке персональных данных, а также определение обязательств, принципов и процедур, которые являются обязательными для физических и юридических лиц, осуществляющих обработку персональных данных.

Турция играет важную роль во многих организациях, либо являясь одним из основателей, либо внося свой вклад в усилия по сотрудничеству в сфере кибербезопасности и информационной безопасности. Поэтому Турция стремится обеспечить кибербезопасность путем обмена информацией и идеями по широкому кругу вопросов с различными странами и организациями, в частности по вопросам разработки политики, наращивания потенциала и обмена информацией.

Поскольку киберпространство не имеет границ, обязательным условием для борьбы с киберугрозами является международное сотрудничество. В этой связи Турция регулярно следит за проведением международных исследований по вопросам кибербезопасности в рамках Организации Объединенных Наций, Организации Североатлантического договора (НАТО), Европейского союза, Организации по безопасности и сотрудничеству в Европе (ОБСЕ) и других международных организаций и институтов и принимает в них участие.

Обеспечение кибербезопасности является также предметом двусторонних соглашений с различными государствами. Министерство транспорта и инфраструктуры, Управление информационно-коммуникационных технологий и Группа по реагированию на чрезвычайные ситуации в компьютерной сфере Турции подписали меморандумы о взаимопонимании по вопросам кибербезопасности с такими государствами, как Босния и Герцеговина, Греция, Грузия, Кыргызстан, Россия, Сербия и Хорватия.

Меморандум о взаимопонимании, посвященный вопросам сотрудничества между НАТО и ее союзниками, был утвержден Комитетом НАТО по киберзащите, который учитывает точку зрения нашего государства, и подписан НАТО и Министерством обороны Турецкой Республики. В соответствии с этим меморандумом о взаимопонимании назначены координаторы и ведется соответствующая работа.

Отслеживается работа Комитета НАТО по планированию на случай чрезвычайных ситуаций гражданского характера и Группы по промышленным ресурсам и коммуникационным услугам. Кроме того, с 2015 года Турция является членом и страной, предоставляющей средства для аккредитованного НАТО аналитического и учебного центра — Экспертного центра НАТО по совместной киберобороне.

Турция участвует в совещаниях Организации экономического сотрудничества и развития, посвященных вопросам безопасности и неприкосновенности частной жизни, и неофициальной рабочей группы ОБСЕ по кибербезопасности и вносит вклад в их работу.

Отслеживается работа совещаний Регионального центра по содействию проверке и осуществлению контроля над вооружениями, и налаживается сотрудничество по различным вопросам. Стратегическая цель Центра заключается в активизации разработки национальных стратегий безопасности путем поощрения регионального сотрудничества и эффективного взаимодействия в области безопасности с целью устойчивого противодействия новым вызовам безопасности, таким как обеспечение кибербезопасности, и другим формам транснациональных угроз, включая терроризм, распространение оружия массового уничтожения, незаконный оборот, организованную преступность, угрозы безопасности границ и пограничному контролю и изменение климата, причем особое внимание будет уделяться всем возникающим угрозам безопасности, обусловленным последней проблемой.

Турция участвует в усилиях по развитию международного сотрудничества. Группа по реагированию на чрезвычайные ситуации в компьютерной сфере Турции является членом Форума групп оперативного реагирования и обеспечения безопасности, сети “Trusted Introducer”, Международного многостороннего партнерства по борьбе с киберугрозами Международного союза электросвязи (МСЭ), платформы НАТО по обмену информацией о вредоносных программах и Альянса кибербезопасности для взаимного прогресса и стремится к максимальному сотрудничеству в целях повышения качества информации о кибербезопасности и обмена опытом и данными об угрозах на международном уровне.

Еще одной важной мерой укрепления сотрудничества и обеспечения готовности является проведение учебных мероприятий по кибербезопасности. Такого рода мероприятия, проводимые на национальном и международном уровнях, способствуют усилению защиты киберпространства и проверке мер, которые необходимо принять для противодействия потенциальным киберугрозам. В этой связи в 2011, 2012, 2013 и 2017 годах в координации с Министерством транспорта и инфраструктуры были проведены национальные учебные мероприятия

по кибербезопасности. 15–16 мая 2014 года в Стамбуле с успехом прошли международные учения по кибербезопасности, которые были организованы в сотрудничестве с МСЭ и его Международным многосторонним партнерством по борьбе с киберугрозами и участие в которых принимали 19 стран.

Турция регулярно принимает участие и оказывает помощь в проведении международных учений по кибербезопасности, таких как «Кибер-коалиция» НАТО, «Сомкнутые щиты» НАТО и учения НАТО по отработке взаимодействия при разрешении кризисных ситуаций.

Поскольку киберпространство не имеет границ, источники и объекты кибератак могут находиться в разных странах, в том числе союзных. Центр командования и управления может находиться в одной стране, а объект нападения — в другой. Поэтому важнейшую роль в борьбе с киберугрозами во всем мире играет обмен информацией о кибератаках и киберпреступниках.

Конвенция о киберпреступности Совета Европы, единственная обязательная к исполнению конвенция по этому вопросу, была открыта для подписания в Будапеште в 2001 году и вступила в силу в 2004 году. Турция подписала Конвенцию в Страсбурге в 2010 году. Конвенция охватывает различные преступления, в частности преступления, совершаемые через Интернет и другие компьютерные сети, мошенничество с использованием компьютерных сетей, детскую порнографию и нарушения безопасности сети, которые в настоящее время включены в национальное законодательство Турции. Кроме того, в уголовном кодексе Турции предусматривается наказание за несанкционированный доступ к информационно-вычислительным системам и несанкционированное вмешательство, перехват, изменение или уничтожение таких систем. Лица, осужденные за эти преступления, наказываются тюремным заключением на срок до трех лет или штрафами. Впоследствии Конвенция была утверждена Законом об утверждении ратификации Конвенции о киберпреступности, а работа по принятию на ее основе национальных законов была завершена в 2016 году.