ГЛОБАЛЬНАЯ КОМИССИЯ
ПО СТАБИЛЬНОСТИ КИБЕРПРОСТРАНСТВА

ЭФФЕКТИВНОЕ ОБЕСПЕЧЕНИЕ КИБЕРСТАБИЛЬНОСТИ

ИТОГОВЫЙ ДОКЛАД
НОЯБРЬ 2019 Г.

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

СТАБИЛЬНОСТЬ В КИБЕРПРОСТРАНСТВЕ КАК УСЛОВИЕ ВСЕОБЩЕГО ПРОЦВЕТАНИЯ И ПОДДЕРЖАНИЯ МИРА

Целью создания Глобальной комиссии по стабильности киберпространства (GCSC) является разработка норм и принципов, призванных повышать безопасность и стабильность киберпространства на международном уровне, а также регулировать деятельность государственных и негосударственных субъектов в киберпространстве.

www.cyberstability.org
info@cyberstability.org | cyber@hcss.nl
@theGCSC

ЭФФЕКТИВНОЕ ОБЕСПЕЧЕНИЕ КИБЕРСТАБИЛЬНОСТИ

ИТОГОВЫЙ ДОКЛАД
НОЯБРЬ 2019 Г.

The Hague Centre for Strategic Studies

***Гаагский* центр стратегических исследований (HCSS)**
Lange Voorhout 1
2514 EA, Гаага

info@hcss.nl
www.hcss.nl

EastWest INSTITUTE

Институт исследований Восток — Запад
Нью-Йорк | Брюссель | Москва | Сан-Франциско

cyber@eastwest.ngo
www.eastwest.ngo

СОПРЕДСЕДАТЕЛИ

Майкл Чертофф (Michael Chertoff), США
Лата Редди (Latha Reddy), Индия
Марина Кальюранд (Marina Kaljurand), Эстония
(бывший председатель)

ЧЛЕНЫ КОМИССИИ

Абдул-Хаким Аджиджола (Abdul-Hakeem Ajijola), Нигерия
Вирджилио Алмейда (Virgilio Almeida), Бразилия
Исаак Бен-Израэль (Isaac Ben-Israel), Израиль
Скотт Чарни (Scott Charney), США
Фредерик Дузе (Frédérick Douzet), Франция
Анриет Эстерхайсен (Anriette Esterhuysen), ЮАР
Джейн Холл Лют (Jane Holl Lute), США
Найджел Инкстер (Nigel Inkster), Великобритания
Ху Бун Хуэй (Khoo Boon Hui), Сингапур
Вольфганг Кляйнвехтер (Wolfgang Kleinwächter), Германия
Олаф Колькман (Olaf Kolkman), Нидерланды
Ли Сяодун (Lee Xiaodong), Китай
Джеймс Льюис (James Lewis), США
Джефф Мосс (Jeff Moss), США
Элина Нур (Elina Noor), Малайзия
Джозеф С. Най — младший (Joseph S. Nye, Jr.), США
Кристофер Пейнтер (Christopher Painter), США
Ури Розенталь (Uri Rosenthal), Нидерланды
Илья Сачков (Ilya Sachkov), Россия
Самир Саран (Samir Saran), Индия
Марьете Шааке (Marietje Schaake), Нидерланды
Мотохиро Цутия (Motohiro Tsuchiya), Япония
Билл Вудкок (Bill Woodcock), США
Чжан Ли (Zhang Li), Китай
Джонатан Зиттрейн (Jonathan Zittrain), США

СПЕЦИАЛЬНЫЕ ПРЕДСТАВИТЕЛИ И СОВЕТНИКИ

Карл Билдт (Carl Bildt), Швеция
Винт Серф (Vint Cerf), США
Сорин Дукару (Sorin Ducaru), Румыния
Марта Финнемор (Martha Finnemore), США

ДИРЕКТОРА

Александр Климбург (Alexander Klimburg), Австрия
Брюс Мак-Коннелл (Bruce W. McConnell), США

ПРЕДСЕДАТЕЛИ НАУЧНО-КОНСУЛЬТАТИВНОЙ ГРУППЫ

Шон Канук (Sean Kanuck), США
Коитиро Комияма (Koichiro Komiyama), Япония
Марилья Масиел (Marília Maciel), Бразилия
Лиис Вихул (Liis Vihul), Эстония
Юго Зильберберг (Hugo Zylberberg), Франция

СЕКРЕТАРИАТ

The Hague Centre for Strategic Studies

EastWest INSTITUTE

ПАРТНЕРЫ

Ministry of Foreign Affairs of the Netherlands

CSA SINGAPORE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

Internet Society

Microsoft

Afilias

СПОНСОРЫ

Министерство иностранных дел Швейцарии

GLOBSEC

Министерство иностранных дел Эстонии

Министерство внутренних дел и коммуникаций Японии

ОРГАНИЗАЦИИ, ОКАЗЫВАЮЩИЕ СОДЕЙСТВИЕ КОМИССИИ

Комиссия Африканского союза

Конференция Black Hat USA

Конференция DEF CON

Представительство Европейского Союза в ООН в Женеве

Глобальный форум по вопросам киберпространства (GFCE)

Google

Муниципалитет Гааги

Packet Clearing House

Тель-Авивский университет

Институт Организации Объединенных Наций по исследованию проблем разоружения

СОДЕРЖАНИЕ

ЗАЯВЛЕНИЕ ПРЕДСЕДАТЕЛЕЙ

Киберпространство — одно из величайших творений человеческой цивилизации, которое существенно изменило характер личных, социальных, экономических и политических взаимоотношений в современном обществе. К сожалению, киберпространство зачастую становится мишенью для разнообразных атак, а иногда и инструментом их осуществления. Поэтому сегодня обеспечение его стабильности становится первоочередной задачей. Концепция стабильности киберпространства во многом близка другой важной концепции — международной стабильности. Для реализации этих концепций необходимо, чтобы все участники геополитического процесса были неизменно привержены делу мира при разрешении разногласий и осуществлении преобразований, которые могут повлиять на стабильность киберпространства, а также осознавали, насколько важно поддерживать такую стабильность.

С самого начала своей работы Глобальная комиссия по стабильности киберпространства исходила из того, что проблема всеобщего мира и безопасности, традиционно отдаваемая на откуп государственным структурам, больше не может решаться без привлечения не связанных с ними организаций и лиц. Киберпространство — это среда, включающая множество участников. В его создании, администрировании и защите от внутренних и внешних угроз на равных участвуют как государственные, так и негосударственные субъекты. Мы стремились отразить это разнообразие при формировании коллектива Комиссии. Помимо лиц, которые ранее занимали высокие государственные посты и решали вопросы международной безопасности, к участию в Комиссии были приглашены ведущие специалисты из таких сфер деятельности, как управление работой Интернета, защита прав человека и развитие сообществ, а также специалисты в области технологий и представители промышленности. В результате в состав Комиссии вошли 28 участников из 16 стран, каждый из которых обладал уникальным опытом и своими взглядами на рассматриваемые нами проблемы. Кроме того, мы вели активный диалог с общественностью и учитывали полученные нами отклики.

Данный отчет является итогом трех лет упорной работы Комиссии. Мы выражаем благодарность всем ее членам, а также нашим советникам и участникам научно-консультативной группы (многие из которых также выступали в качестве волонтеров), спонсорам и совету директоров. Без них работа Комиссии была бы невозможна. Наконец, мы обязаны упомянуть представителей секретариата, которые не только активно способствовали учреждению Комиссии как общественной инициативы, но и умело координировали ее работу.

Комиссия также принимала во внимание прочие программы по анализу проблем киберпространства — как завершенные, так и активные. Наш доклад *Эффективное обеспечение киберстабильности* дополняет эти программы и помогает их осуществлению, а также содержит новые предложения, призванные обеспечить стабильность киберпространства.

Майкл Чертофф
Сопредседатель
Глобальная комиссия
по стабильности
киберпространства

Лата Редди
Сопредседатель
Глобальная комиссия
по стабильности
киберпространства

КРАТКОЕ СОДЕРЖАНИЕ ДОКЛАДА

На сегодняшний день период стратегической стабильности и относительного мира между крупными державами, длившийся двадцать пять лет, подошел к концу. Конфликт между государствами приобрел новые формы, и дестабилизация мирового сообщества в немалой степени обусловлена деятельностью в киберпространстве. За последнее десятилетие кибератаки со стороны государственных и негосударственных структур стали более частыми и изощренными. Это ставит стабильность киберпространства под угрозу. Проще говоря, люди и организации больше не могут быть уверены в своей безопасности при работе в киберпространстве, а также в стабильности и неприкосновенности сервисов или данных.

В связи с этим различные частные лица и организации приняли решение создать Глобальную комиссию по стабильности киберпространства (GCSC), которая могла бы выработать рекомендации, обеспечивающие безопасность в Интернете. Отправной точкой в работе комиссии стало формулирование концепции киберстабильности. Данная концепция состоит из семи компонентов: 1) многостороннее сотрудничество; 2) принципы киберстабильности; 3) разработка и исполнение норм, применяемых на добровольной основе; 4) соблюдение принципов международного права; 5) меры по укреплению доверия; 6) наращивание потенциала; 7) открытое распространение и широкое использование технических стандартов, обеспечивающих устойчивость киберпространства. Сформулировав данную концепцию, комиссия подробно изучила три из семи перечисленных компонентов, а именно многостороннее сотрудничество, принципы и нормы.

Несмотря на то, что многостороннее сотрудничество является обязательным условием реализации различных международных договоров, возможность его достижения остается предметом споров. До сих пор распространено мнение, что обеспечение международной безопасности и стабильности в подавляющем большинстве случаев является обязанностью государственных структур. Однако на практике киберпространство является как результатом деятельности, так и полем конкуренции преимущественно негосударственных субъектов и мы считаем, что для обеспечения стабильности киберпространства необходимо активно взаимодействовать с ними. Более того, их участие в этом процессе неизбежно, поскольку зачастую именно они либо находятся на переднем крае борьбы с киберугрозами, либо являются их источником.

Комиссия пришла к выводу, что, поскольку эти негосударственные субъекты играют решающую роль в обеспечении стабильности киберпространства, на их деятельность также должны распространяться определенные принципы и нормы. Данная точка зрения нашла свое отражение в следующих четырех принципах, призывающих все стороны проявлять ответственность, разумно ограничивать свои действия, вмешиваться, когда этого требует ситуация, и уважать права человека.

- Ответственность: каждый участник процесса несет ответственность за сохранение стабильности киберпространства.
- Дисциплина: государственные и негосударственные субъекты не должны предпринимать действия, которые ставят стабильность киберпространства под угрозу.
- Необходимое вмешательство: государственные и негосударственные субъекты должны принимать разумные и надлежащие меры для обеспечения стабильности киберпространства.
- Уважение прав человека: усилия по обеспечению стабильности киберпространства не должны нарушать права человека и верховенство закона.

Опираясь на эти принципы и стремясь дополнить результаты других программ (при этом не дублируя их), Комиссия разработала восемь норм, которые призваны укрепить стабильность киберпространства и устранить технические недочеты или пробелы в прежних нормах.

1. Государственные и негосударственные субъекты не должны вести или сознательно допускать деятельность, которая преднамеренно наносит существенный ущерб общедоступности или целостности ядра Интернета и, как следствие, стабильности киберпространства.
2. Государственные и негосударственные субъекты не должны проводить, поддерживать или допускать кибероперации, направленные на нарушение нормальной работы технической инфраструктуры, необходимой для проведения выборов, референдумов или плебисцитов.
3. Государственные и негосударственные субъекты не должны вмешиваться или допускать вмешательство в разработку и производство товаров и услуг, если такое вмешательство может существенно нарушить стабильность киберпространства.

4. Государственные и негосударственные субъекты не должны распоряжаться ресурсами ИКТ широкой общественности для использования в качестве ботнетов или для аналогичных целей.

5. Государства должны создать прозрачные с процедурной точки зрения методики, позволяющие оценивать, когда следует (и следует ли) сообщать общественности об уязвимостях или недостатках информационных систем или технологий. По умолчанию подобные сведения всегда следует обнародовать.

6. Разработчики и производители товаров и услуг, от которых зависит стабильность киберпространства, должны: 1) в первую очередь руководствоваться соображениями безопасности и стабильности; 2) предпринимать экономически обоснованные шаги с целью гарантировать, что в их продукции нет существенных уязвимостей; 3) своевременно устранять недоработки при последующем обнаружении таковых, осуществляя свою деятельность на условиях прозрачности. Все участники обязаны обмениваться информацией об уязвимостях, чтобы помочь предотвратить или смягчить злонамеренную киберактивность.

7. Государства должны принимать соответствующие меры, в том числе утверждать законы и правовые нормы, которые будут гарантировать элементарную гигиену киберпространства.

8. Негосударственные субъекты не должны участвовать в атакующих кибероперациях, а государственные структуры должны предотвращать подобные действия и реагировать в тех случаях, если они совершаются.

Рекомендации

Признавая важность многостороннего сотрудничества и отдавая себе отчет в том, что объявление того или иного действия обязательным не всегда делает его таковым, комиссия разработала указанные ниже шесть рекомендаций, которые призваны воплотить в жизнь модель многостороннего сотрудничества, стимулировать признание и исполнение норм, а также гарантировать ответственность субъектов, эти нормы нарушающих.

Этих рекомендации приведены ниже в краткой форме.

1. Государственные и негосударственные субъекты должны признавать и внедрять нормы, которые предотвращают дестабилизирующие действия и стимулируют надлежащие меры для укрепления стабильности киберпространства.

2. Действуя в рамках своих обязанностей и ограничений, государственные и негосударственные субъекты должны соответствующим образом реагировать на нарушения выработанных норм, чтобы за такими нарушениями следовали ожидаемые и ощутимые карательные меры.

3. Государственные и негосударственных субъекты, включая международные организации, должны наращивать усилия по обучению специалистов, расширению потенциала в сфере кибербезопасности и широкому распространению информации о том, почему важна стабильность киберпространства. При этом должны учитываться разнородные потребности участвующих сторон.

4. Государственные и негосударственные субъекты должны собирать, анализировать и публиковать сведения о нарушениях норм и последствиях таких нарушений.

5. Государственные и негосударственные субъекты должны создавать и поддерживать заинтересованные сообщества, тем самым содействуя сохранению стабильности киберпространства.

6. Для решения проблем стабильности должен быть создан постоянный механизм многостороннего сотрудничества, позволяющий государственным лицам, частному сектору (в том числе представителям сферы технологий) и представителям гражданского общества участвовать в принятии решений и обмениваться мнениями.

Публикация данного отчета знаменует собой как окончание одного этапа работы, так и начало другого. Комиссия выполнила возложенные на нее задачи, и ее миссия завершена. Но для членов Комиссии и ее помощников, а также всех тех, кто способствовал ее деятельности, кропотливая работа по претворению этих принципов, норм и рекомендаций в жизнь только начинается. Откладывать эту работу никак нельзя, потому что если мы не обеспечим стабильность киберпространства, то утратим все преимущества, которые оно может нам предложить.

1. ВВЕДЕНИЕ

Эволюция цифровых технологий и развитие киберпространства кардинально изменили нашу жизнь [1]. Возможность хранить, анализировать и отправлять в любую точку мира информацию в цифровом формате существенным образом затронула все аспекты жизни общества и значительно изменила характер личных, деловых и политических взаимоотношений. На сегодняшний день около половины населения Земли имеет доступ в Интернет [2], и этот показатель стремительно растет. При этом даже лица, не использующие интернет-технологии, оказываются в зависимости от них, поскольку организации, обеспечивающие население товарами и услугами, зачастую пользуются возможностями киберпространства для обмена информацией, а также управления транспортом и финансами.

Возможности, которые нам дает киберпространство, и необходимость обеспечения его стабильности неоднократно становились предметом дискуссий, поскольку эта тема является проблемной. Главная трудность состоит в том, что киберпространство можно использовать как во благо, так и во вред. Благодаря повсеместному распространению каналов для соединения с Интернетом, их анонимности, а также недостаточно эффективным средствам отслеживания пользователи и устройства могут подключаться к базам данных и различным системам без предоставления каких-либо идентифицирующих сведений. Эти же особенности киберпространства позволяют злоумышленникам совершать преступления и оставаться безнаказанными. В результате правительства, организации и люди по всему миру оказываются перед непростым выбором. Правительства заинтересованы в защите киберпространства, предоставлении государственных услуг и стимулировании прочих общественно важных видов деятельности (таких как образование и интернет-банкинг), но в то же время они хотят использовать возможности киберпространства в интересах национальной безопасности, например, для расширения возможностей правоохранительных, разведывательных и военных органов. Организации, которые хотят защитить своих клиентов, деловую репутацию и доходы, вынуждены противостоять атакам, заниматься расследованием подозрительных действий и отвечать на запросы государства о предоставлении данных. По мере того как цифровые технологии все глубже проникают в повседневную жизнь, любой человек оказывается все более зависим от них, невзирая на то, пользуется ли он Интернетом или нет. В результате целостность киберпространства и доступ к нему оказываются все более и более важными. За последнее десятилетие кибератаки, в том числе нацеленные на государственные организации и объекты инфраструктуры, стали более частыми и изощренными [3]. Таким образом, ни текущее положение дел, ни тенденции обозримого будущего не внушают оптимизма.

Кибератаки, осуществляемые как государственными, так и негосударственными субъектами, ясно дают понять, что реализация концепции киберстабильности является насущной потребностью в мировом масштабе. Данная концепция призвана уменьшить вероятность значительных нарушений в работе киберпространства, которые могут свести на нет его преимущества и поставить под угрозу благосостояние людей, в том числе их права и свободы. Очевидно, что, когда разработке товаров и услуг уделяется должное внимание, когда ИТ-специалисты и пользователи компьютеров обращаются с

1 Понятие киберпространства имеет несколько определений. См. https://ru.wikipedia.org/wiki/Киберпространство. Из словаря: «Киберпространство — это электронная система, позволяющая пользователям компьютеров по всему миру общаться друг с другом или получать доступ к информации с любой целью». См. https://dictionary.cambridge.org/us/dictionary/english/cyberspace. В Великобритании под термином «киберпространство» подразумеваются электронные средства связи в формате цифровых сетей, используемые для хранения, изменения и передачи информации. К ним относится Интернет, а также прочие информационные системы, необходимые для функционирования организаций или инфраструктурных объектов и предоставления услуг. См. https://www.cpni.gov.uk/cyber. В этом смысле понятие киберпространства является более широким, чем понятие Интернета, которое определяется как глобальная система взаимосвязанных компьютерных сетей, в которой для связи между устройствами по всему миру используется набор интернет-протоколов (TCP/IP). См. https://ru.wikipedia.org/wiki/Интернет. См. также дискуссионную статью Международного союза электросвязи «Определение понятия Интернета» (Defining the Internet, май 2013 г.): https://www.itu.int/dms_pub/itu-s/md/13/wtpf13/inf/S13-WTPF13-INF-0008%21%21MSW-E.docx.

2 Статистика использования Интернета, данные Internet World Stats за 4 октября 2019 г.: https://internetworldstats.com/stats.htm.

3 Центр стратегических и международных исследований (CSIS), *Значительные киберинциденты с 2006 г.* (Significant Cyber Incidents Since 2006). См. https://csis-prod.s3.amazonaws.com/s3fs-public/190904_Significant_Cyber_Events_List.pdf; Луис Маринос (Louis Marinos) и Марко Лоуренцо (Marco Lourenço), ред., *Отчет ENISA по уровню угроз на 2018 г.* (ENISA Threat Landscape Report 2018), январь 2019 г.: https://www.enisa.europa. eu/publications/enisa-threat-landscape-report-2018; Абишек Агравал (Abhishek Agrawal) и др., *Аналитический отчет Майкрософт о безопасности, выпуск 24* (Microsoft Security Intelligence Report, Vol. 24), декабрь 2018 г.: https://clouddamcdnprodep.azureedge.net/gdc/gdc09FrGq/original; ООН, Генеральная Ассамблея, *Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: доклад Генерального секретаря*, A/74/120, 24 июня 2019 г.: https://undocs.org/ru/A/74/120.

этими товарами и услугами надлежащим образом, безопасность и стабильность киберпространства повышаются. И наоборот — безответственные действия разработчиков или беспечное обращение с технологиями могут привести к дестабилизации и уязвимости киберпространства. Однако в условиях, когда государственные и негосударственные субъекты рассматривают Интернет как поле боя, где каждый может отвоевать себе политическое, военное или экономическое преимущество, одной только оптимизацией процессов разработки и эксплуатации не обойтись. Как бы ни была хороша защита, достаточно упорный злоумышленник найдет способ ее обойти. Поэтому часто можно услышать мнение, что в Интернете лучшая защита — нападение. Это порождает нестабильность [4]. Таким образом, важно делать акцент не только на технологическом аспекте, но и на поведенческом. Возникает вопрос: как побудить всех субъектов действовать добросовестно, чтобы стабильность киберпространства усиливалась, а не ослабевала?

Для ответа на этот вопрос ряд правительственных и неправительственных организаций учредили Глобальную комиссию по стабильности киберпространства (GCSC) [5], задача которой была сформулирована следующим образом.

> На сегодняшний день период стратегической стабильности и относительного мира между крупными державами, длившийся двадцать пять лет, подошел к концу. Конфликт между государствами приобрел новые формы, и дестабилизация мирового сообщества в немалой степени обусловлена деятельностью в киберпространстве. В результате под угрозой оказывается сама возможность мирного использования киберпространства в целях стимулирования экономического роста и распространения гражданских свобод.
>
> В рамках противодействия этим тенденциям Глобальная комиссия по стабильности киберпространства берет на себя разработку норм и принципов, призванных повышать безопасность и стабильность киберпространства на международном уровне, а также регулировать деятельность государственных и негосударственных субъектов в киберпространстве. Чтобы достичь общего понимания по стоящим перед ней задачам, Комиссия намерена сотрудничать с широким кругом заинтересованных лиц. Цель своей работы она видит в укреплении киберстабильности путем повышения информированности общества, наращивания научно-технического потенциала, проведения исследований и пропагандирования своих принципов [6].

Стоит отметить, что комиссия представляет собой наглядный пример глобального многостороннего сотрудничества, поскольку в ее состав входят представители самых разных сфер деятельности. Некоторые члены комиссии ранее занимали правительственные посты и лично участвовали в двусторонних и многосторонних переговорах по вопросам кибербезопасности. Другие много лет занимались созданием, обслуживанием и защитой непосредственно инфраструктуры Интернета. Третьи выступали в роли представителей гражданского общества.

Отдавая себе отчет в том, что, помимо данной комиссии, проблемами киберпространства занимались и занимаются самые разные учреждения и объединения, мы стремились учесть все актуальные исследования в области киберпространства, чтобы избежать дублирования результатов этих исследований. В своей работе мы стремились дополнить и расширить существующие процессы многостороннего сотрудничества и государственного содействия. К таким процессам относится фундаментальная деятельность Группы правительственных экспертов Организации Объединенных Наций (ГПЭ ООН) [7], работа организаторов и участников Глобального форума по

4 Например, см. статью «Культ кибервойны» (The Cult of the Cyber Offensive) П. У. Сингера (P.W. Singer) и Аллана Фридмана (Allan Friedman) в журнале *Foreign Policy*, 15 января 2014 г.: https://foreignpolicy.com/2014/01/15/cult-of-the-cyber-offensive/; Всемирный экономический форум (ВЭФ), *Отчет о глобальных рисках 2019* (The Global Risks Report 2019), 2019 г.: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf.

5 Более подробные сведения о комиссии см. в приложении В, «История создания Комиссии, методы ее работы и стоящие перед ней задачи».

6 Глобальная комиссия по стабильности киберпространства: https://cyberstability.org/.

7 В 2015 г. Генеральная Ассамблея ООН приняла важную резолюцию, в которой единогласно подтвердила, что ГПЭ ООН выполнила поставленные перед ней задачи. См. резолюцию Генеральной Ассамблеи ООН 70/237 *Резолюция, принятая Генеральной Ассамблеей 23 декабря 2015 года [по докладу Первого комитета (A/70/455)]*: https://undocs.org/ru/A/RES/70/237. Таким образом, международное право и, в частности, Устав ООН определяют исчерпывающую методику международного реагирования на враждебные действия, которая применима и к кибероперациям. Наша работа базируется на приверженности всех стран — участников Генеральной Ассамблеи ООН 2015 г. принципам ответственного поведения с целью укрепить стабильность и безопасность при использовании ИКТ, а также обязательствам в отношении добросовестного исполнения норм и сотрудничества.

вопросам киберпространства (GFCE) [8], Всемирной встречи на высшем уровне по вопросам информационного общества (WSIS), Форума по управлению Интернетом (IGF), Глобальной конференции по вопросам киберпространства (GCCS, London Process), а также участников инициативы NETmundial, Хартии доверия (Charter of Trust), Технологического соглашения по кибербезопасности (Cybersecurity Tech Accord) и Парижского призыва к доверию и безопасности в киберпространстве (он же Парижский призыв), деятельность Рабочей группы открытого состава ООН, Глобальной комиссии по управлению Интернетом (Global Commission on Internet Governance, она же Комиссия Билдта), Организации по безопасности и сотрудничеству в Европе (ОБСЕ), Комиссии Африканского союза (она же Комиссия АС), Гаагской платформы по разработке норм поведения в киберпространстве (The Hague Program for Cyber Norms), Института Организации Объединенных Наций по исследованию проблем разоружения (ЮНИДИР), а также Группы высокого уровня Генерального секретаря по цифровому сотрудничеству ООН. Кроме того, мы вели активный диалог с общественностью и учитывали ее мнение, а также пользовались результатами выполненных по заказу Комиссии исследований.

Некоторые из приведенных выше организаций и объединений занимались, помимо прочего, вопросами стабильности киберпространства. Одна из проблем, которую они пытались решить, заключалась в тесной связи между стабильностью киберпространства и управляющими им механизмами. Суть в том, что в отсутствие эффективной модели управления общество не в состоянии обеспечить стабильность киберпространства, поскольку у него отсутствуют необходимые для этого средства взаимодействия и принятия решений. В частности, Комиссия Билдта разработала многосторонний общественный договор, призванный, по словам ее представителей, обеспечить конфиденциальность и безопасность в цифровой среде при взаимодействии «между гражданами и их избранными представителями, судебными, правоохранительными и разведывательными органами, коммерческими организациями, членами гражданского и технологического интернет-сообщества с целью восстановления и укрепления доверия по отношению к Интернету» [9].

Мы высоко ценим работу, проделанную нашими предшественниками, которым пришлось разрабатывать принципы, правила и нормы для хаотичной среды, какой являлось только появившееся киберпространство. Однако если мы хотим укрепить стабильность киберпространства, нам нужна единая всесторонняя концепция. Мы знаем по примерам из истории, что на разработку механизмов контроля над принципиально новыми и потенциально опасными технологиями у правительств и сообществ иногда уходят десятилетия [10]. Киберпространство стало одним из важнейших аспектов взаимозависимости глобальной экономики, общественного развития и безопасности лишь с распространением доступа к Всемирной паутине в конце 1990-х гг. Это значит, что процессы управления им все еще находятся на ранних стадиях формирования и при этом не все необходимые правовые нормы разработаны в равной степени [11]. Например, у нас есть четко сформулированные требования законодательства и эффективные структуры, регулирующие использование службы доменных имен, в то время как вопросы регулирования контента являются поводом для существенных разногласий между организациями и государствами. Иногда государственные и негосударственные субъекты применяют для регулировки киберпространства положения законодательства из других сфер, таких как торговля или интеллектуальная собственность. Частные же компании все чаще и чаще разрабатывают свои собственные нормы [12]. Комиссия не ставит перед собой задачу систематизировать все возможные подходы к управлению Интернетом. Наша миссия — разработать такую общую концепцию, которая охватила бы все эти подходы и тем самым позволила обеспечить стабильность киберпространства.

От нашего внимания также не ускользнуло, что те, кто пытается решить проблему стабильности киберпространства, зачастую не могут угнаться за теми, кто пытается эту стабильность расшатать, а также за технологическими нововведениями и изменениями в геополитических расстановках. Это связано, в первую очередь, с тем, что с появлением киберпространства субъекты стали использовать иные средства для достижения политических и военных целей. Нарастить военную мощь в киберпространстве гораздо проще, чем в реальности, и многие решили этим воспользоваться. Кроме того, получив доступ к новым возможностям, такие субъекты не спешат ограничивать себя, особенно если другие участники процесса также пренебрегают ограничениями. Международное сообщество нуждается в единой всеобщей концепции киберстабильности, которая не только позволит навести необходимый порядок, но и не устареет в результате стремительного развития технологий. Защита стабильности киберпространства — это главная цель, с определения которой начинается наша работа.

8 Одним из ключевых направлений деятельности Глобальной комиссии по стабильности киберпространства было наращивание потенциала. См., например, «Итоговое заявление по глобальной повестке GFCE в отношении наращивания киберпотенциала», Дели (Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building), Глобальный форум по вопросам киберпространства, 24 ноября 2017 г.: https://www.thegfce.com/delhi-communique/documents/publications/2017/11/24/delhi-communique.

9 Глобальная комиссия по управлению Интернетом, *Единый Интернет* (One Internet), ч. IX, 2016 г.: https://www.cigionline.org/sites/default/files/gcig_final_report_-_with_cover.pdf. «Мы призываем всех и каждого — правительства, частные корпорации, гражданское сообщество, технологическое сообщество, обычных людей — объединиться и вместе создать новый общественный договор для цифровой эпохи».

10 Возможно, одним из наиболее релевантных примеров управляющей структуры подобного типа является структура контроля над ядерными вооружениями, формирование которой потребовало времени и усилий. Даже сейчас, 60 лет спустя после принятия Договора о нераспространении ядерного оружия, проблема такого контроля по-прежнему вызывает опасения.

11 Этот ранний этап получил название «набор систем». См. статью «Набор систем для управления системными международными кибероперациями» (The Regime Complex for Managing Complex Global Cyber Activities), Джозеф Най, Глобальная комиссия по управлению интернетом, № 1 май 2014 г.: https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.

12 Например, см. нормы, разработанные ISOC и Майкрософт: Соглашение MANRS (Mutually Agreed Norms for Routing Security), Internet Society (2014 г.), https://www.manrs.org/; Анджела МакКей (Angela McKay) и др., *Снижение напряженности в зависимом от Интернета мире за счет внедрения международных норм кибербезопасности* (International Cybersecurity Norms Reducing Conflict in an Internet-dependent World), Microsoft, декабрь 2014 г.: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVroA; и Скотт Чарни (Scott Charney) и др., *От формулировки к внедрению: продвижение в контексте работы над нормами кибербезопасности* (From Articulation to Implementation: Enabling Progress on Cybersecurity Norms), Microsoft, июнь 2016 г.: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8.

2. ЧТО ТАКОЕ СТАБИЛЬНОСТЬ КИБЕРПРОСТРАНСТВА?

ОПРЕДЕЛЕНИЕ

Стабильность киберпространства определяется как ситуация, когда все пользователи вполне уверены в том, что они могут пользоваться возможностями киберпространства безопасным и надежным образом, что доступность и целостность данных и сервисов в киберпространстве в общем и целом гарантирована, что управление переменами происходит сравнительно мирно и что возникающие противоречия регулируются без их эскалации.

Данное определение, сформулированное комиссией, основано на стандартном определении понятия «стабильность» [13], но оно дополнено двумя важными уточнениями. Во-первых, в нем упоминается такой фактор, как уверенность пользователей. Это особенно важно, поскольку люди принимают решения, основываясь на своем восприятии, а не только на объективных фактах и, если пользователь воспринимает киберпространство как нестабильное, он может отказаться от его использования и, таким образом, упустить преимущества, которые оно может дать. Например, использование возможностей киберпространства может помочь оптимизировать процессы и повысить их эффективность. Из этого можно сделать вывод, что определенные системы (такие как системы доступа к государственным услугам и онлайн-банкингу) могли бы существенно выиграть за счет использования этих возможностей. Однако если подобные системы являются ненадежными (или воспринимаются как таковые), они не получат должного распространения и возможности, предоставляемые технологией киберпространства, окажутся упущены.

Во-вторых, следует помнить, что киберпространство — это сфера, в которой постоянно что-то меняется, будь то технологии, бизнес-модели, функциональность или же представления о том, какую роль должны играть технологии в повседневной жизни общества. Таким образом, в отличие от словарного определения понятия «стабильность», включающего возвращение к исходному состоянию, в случае с киберпространством мы имеем дело с постоянно развивающимися технологиями, и потому для обеспечения киберстабильности нам нужны гибкие, адаптивные механизмы. Проще говоря, пользователи должны оставаться уверены в доступности и целостности киберпространства, даже если в нем — и в окружающем нас реальном мире — происходят перемены.

13 Стабильность определяется как «пребывание в стабильном состоянии»: https://www.lexico.com/en/definition/stability. Термин «стабильный» может означать следующее: 1) не подверженный смещению или опрокидыванию, надежно закрепленный; 2) не подверженный изменениям или сбоям, твердо устоявшийся; 3) не подверженный физическим изменениям. См. https://en.oxforddictionaries.com/definition/stable. В рамках международных отношений можно упомянуть следующее определение понятия «международная стабильность», являющееся одним из наименее противоречивых: «вероятность того, что [международная] система сохранит все свои основные свойства, что ни одно государство не займет доминирующее положение, что большинство участников системы продолжат существование и что не возникнет крупномасштабная война». Цитируется по статье Карла В. Дойча и Дж. Дэвида Сингера «Многополярная система власти и международная стабильность» (Karl W. Deutsch and J. David Singer, ultipolar Power Systems and International Stability), *World Politics*, ч. 16, № 3, апрель 1964 г., 390–406,http://users.metu.edu.tr/utuba/Deutsch.pdf

3. КОНЦЕПЦИЯ КИБЕРСТАБИЛЬНОСТИ, ПРЕДЛАГАЕМАЯ КОМИССИЕЙ

Для решения описанных выше проблем Комиссия, следуя примерам других организаций [14], предлагает всеобщую концепцию киберстабильности. Она предусматривает следующее: 1) многостороннее сотрудничество; 2) принципы киберстабильности; 3) разработку и исполнение норм, применяемых на добровольной основе; 4) соблюдение принципов международного права; 5) меры по укреплению доверия; 6) наращивание потенциала; 7) открытое распространение и широкое использование технических стандартов, обеспечивающих устойчивость киберпространства. Усилия Комиссии были сосредоточены в первую очередь на трех из перечисленных аспектов — многостороннем сотрудничестве, принципах и законодательных нормах, которые рассматриваются в разделах 4, 5 и 6 соответственно. Что касается норм, то мы уделили внимание не только их разработке, но и более сложным проблемам, связанным с их принятием и внедрением, а также ответственности за их нарушение.

Мы обращаем внимание на то, что в настоящее время многие организации предпринимают немало усилий по реализации отдельных компонентов нашей концепции киберстабильности, но эти усилия, подобно самому киберпространству, носят децентрализованный характер. Наша Комиссия полагает, что воплотить эту концепцию в жизнь можно будет только согласованными усилиями многих заинтересованных сторон в глобальном масштабе. Поэтому Комиссия занимается не только концептуальными вопросами, но и вырабатывает практические рекомендации, призванные реализовать и дополнить наработки, достигнутые в рамках других программ, и, по возможности, вдохнуть в них новую энергию.

14 См., например, *Век цифровой взаимозависимости: доклад группы высокого уровня Генерального секретаря ООН по цифровому сотрудничеству,* стр. 5, июнь 2019 г.: https://digitalcooperation.org/wp-content/uploads/2019/06/HLP-on-Digital-Cooperation-Report-Executive-Summary-RU.pdf. Цитата: «Мы рекомендуем разработать глобальные обязательства по цифровому доверию и безопасности для формирования общего представления, определения признаков цифровой стабильности, разъяснения и усиления внедрения норм ответственного использования технологий, а также внести предложения по приоритетным действиям».

4. МНОГОСТОРОННЕЕ СОТРУДНИЧЕСТВО

Хотя важность многостороннего сотрудничества систематически декларируется во многочисленных международных соглашениях, оно до сих пор остается предметом дискуссий. Одни участники таких дискуссий воспринимают их как отвлеченные и концентрируются в основном на том, какую роль играют государственные и негосударственные субъекты в международных отношениях и регулировании технологического сектора. Другие рассматривают процессы многостороннего сотрудничества с практической точки зрения, полагая, что государства, действующие в одиночку или при минимальном участии негосударственных структур, не могут обеспечить стабильность киберпространства [15]. Мы разделяем второй подход.

Дискуссии о преимуществах вовлечения различных заинтересованных сторон в процесс решения назревших проблем длятся уже не одно десятилетие. Эта тема неоднократно возникала при обсуждении проблем управления Интернетом, но в то же время она неизменно связана с вопросами правовых норм и национальной безопасности. Например, в ходе второго этапа Всемирной встречи на высшем уровне по вопросам информационного общества (WSIS) Рабочая группа ООН по управлению Интернетом (WGIG) отвергла концепцию единоличного руководства. Напротив, она пришла к выводу, что Интернет слишком велик, чтобы им могла управлять одна группа заинтересованных сторон или одна организация, и предложила применять многосторонний подход. В 2005 г. главы государств Тунисской программы WSIS выступили со следующим заявлением: «Рабочее определение управления использованием Интернета означает разработку и применение правительствами, частным сектором и гражданским обществом в рамках исполнения ими соответствующих ролей общих принципов, норм, правил, процедур принятия решений и программ, которые формируют условия для развития и использования Интернета» [16].

Такая же точка зрения была высказана десятью годами позже в ходе совещания высокого уровня Генеральной Ассамблеи ООН, посвященного проблеме реализации решений Всемирной встречи на высшем уровне по вопросам информационного общества. В частности, эта позиция отражена в резолюции Генеральной Ассамблеи ООН 70/125 от 16 декабря 2015 г.:

> «Мы вновь подтверждаем, кроме того, ценность и принципы сотрудничества и взаимодействия широкого круга заинтересованных сторон, которые с самого начала характеризуют процесс осуществления решений Всемирной встречи на высшем уровне по вопросам информационного общества, признавая, что эффективное участие правительств, частного сектора, гражданского общества, международных организаций, технических и научных кругов и всех других соответствующих заинтересованных сторон в рамках их функций и обязанностей, особенно при сбалансированной представленности развивающихся стран, имело и по-прежнему имеет исключительно большое значение для развития информационного общества» [17].

15 «В определении Всемирной встречи на высшем уровне по вопросам информационного общества, которое было сформулировано в 2005 г., вводится понятие соответствующих ролей и провозглашается принцип общего подхода. В декларации конференции NETmundial (2014 г.) были изложены такие ключевые принципы, как организация «снизу вверх», открытость, прозрачность, инклюзивность и соблюдение прав человека. Другими словами, у нас есть некие общие принципы многостороннего подхода, но нет единой модели участия многих заинтересованных сторон. На сегодняшний день сложились две подобные модели: консультативная модель и модель сотрудничества». Вольфганг Кляйнвехтер, «На пути к целостному подходу при формировании государственной политики в области Интернета» (Wolfgang Kleinwächter, Towards a Holistic Approach for Internet Related Public Policy Making), Глобальная комиссия по стабильности киберпространства, январь 2018 г: https://cyberstability.org/wp-content/uploads/2018/02/GCSC_Kleinwachter-Thought-Piece-2018-1.pdf. С дополнительными материалами по дискуссиям о моделях с участием многих заинтересованных сторон можно ознакомиться в статье Вирджилио Алмейды и др. «Происхождение и эволюция моделей с участием многих заинтересованных сторон» (Virgilio Almeida et al., The Origin and Evolution of Multistakeholder Models), *IEEE Internet Computing*, ч. 19, январь-февраль 2015 г., 74–79, https://doi.ieee-computersociety.org/10.1109/MIC.2015.15.

16 «Тунисская программа для информационного общества», материалы Всемирной встречи на высшем уровне по вопросам информационного общества, п. 34, 18 ноября 2005 г.: https://www.itu.int/net/wsis/docs2/tunis/off/6rev1-ru.html.

17 См. резолюцию Генеральной Ассамблеи ООН 70/125, *Итоговый документ совещания высокого уровня Генеральной Ассамблеи, посвященного общему обзору хода осуществления решений Всемирной встречи на высшем уровне по вопросам информационного общества*, A/RES/70/125, п. 3, 16 декабря 2015 г.: https://undocs.org/ru/A/RES/70/125.

Снова обратим внимание на то, что поднимаемые в документе темы не ограничиваются проблематикой управления ключевыми интернет-ресурсами и непосредственно касаются вопросов национальной безопасности:

> «Мы признаем ведущую роль правительств в вопросах кибербезопасности, связанных с национальной безопасностью. Мы признаем далее важную роль всех заинтересованных сторон и вклад, вносимый ими в соответствии со своими функциями и обязанностями» [18].

Что касается непосредственно вопроса правовых норм, то в 2011 г. представители «Большой восьмерки» (G8) заявили по этому поводу следующее:

> «Безопасность сетей и сервисов в Интернете — это вопрос, касающийся многих заинтересованных сторон. Его решение требует скоординированных усилий со стороны правительственных структур, региональных и международных организаций, частного сектора и гражданского общества... Правительства при взаимодействии со всеми другими заинтересованными сторонами должны заниматься разработкой правовых норм, регулирующих поведение в киберпространстве, и общих подходов к его использованию» [19].

Двумя годами позже, в 2013 г., Группа правительственных экспертов (ГПЭ) ООН опубликовала документ под названием *Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности*. В разделе «Укрепление сотрудничества в целях создания мирной, безопасной, устойчивой и открытой информационной среды» представители ГПЭ ООН высказывают следующие соображения: «...[хотя] государства должны играть лидирующую роль в решении указанных вопросов, вместе с тем активное участие частного сектора и гражданского общества могло бы способствовать повышению эффективности сотрудничества» [20]. Далее в разделе «Рекомендации в отношении норм, правил и принципов ответственного поведения государств», говорится следующее:

> «Государствам-членам следует изыскивать оптимальные формы сотрудничества в области осуществления вышеупомянутых норм и принципов ответственного поведения с учетом потенциальной роли частного сектора и организаций гражданского общества» [21].

Эти позиции были подтверждены в докладе ГПЭ ООН за 2015 г., который содержит следующие заявления:

> «Государства несут главную ответственность за поддержание безопасной и мирной ИКТ-среды, однако определение механизмов участия, сообразно обстоятельствам, частного сектора, научных кругов и организаций гражданского общества могло бы способствовать повышению эффективности международного сотрудничества» [22].

Это положение было повторено в резолюции Генеральной Ассамблеи ООН от 2018 г., посвященной такой теме, как *Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности* [23]. Подобная точка зрения ясно выражена и в других международных соглашениях. Вот что гласит, например, Парижский призыв: «Мы признаем необходимость оптимизированного подхода с привлечением большого количества участников, а также дополнительных усилий для снижения рисков, угрожающих стабильности киберпространства, и укрепления надежности, потенциала и доверия» [24].

---

18 Там же, п. 50.

19 Декларация «Большой восьмерки»: «Неизменная приверженность свободе и демократии», Довильский саммит «Большой восьмерки», п. 17, 27 мая 2011 г.: http://kremlin.ru/supplement/946.

20 Генеральная Ассамблея ООН, *Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности*, A/68/98, стр. 9, п. 12, 24 июня 2013 г. (далее — Доклад ГПЭ ООН 2013): https://undocs.org/ru/A/68/98.

21 Там же, стр. 11, п. 25.

22 Генеральная Ассамблея ООН, *Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности*, A/70/174 (a), стр. 17, п. 31, 22 июля 2015 г. (далее — Доклад ГПЭ ООН 2015): https://undocs.org/ru/A/70/174.

23 Резолюция Генеральной Ассамблеи ООН 73/266 *Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности*, A/RES/73/266, 22 декабря 2018 г.: https://undocs.org/ru/A/RES/73/266.

24 Министерство по делам Европы и иностранных дел Франции, «Парижский призыв к доверию и безопасности в киберпространстве», 11 ноября 2018 г.: https://www.diplomatie.gouv.fr/IMG/pdf/appel_de_paris_en_russe_cle8a41ae.pdf. См. также «Заявление NETmundial об участии многих заинтересованных сторон» (NETmundial, NETmundial Multistakeholder Statement), 24 апреля 2014 г.: http://netmundial.br/wp-content/up-loads/2014/04/NETmundial-Multistakeholder-Document.pdf.

Совсем недавно, в июне 2019 г., был опубликован доклад группы высокого уровня Генерального секретаря ООН по цифровому сотрудничеству *Век цифровой взаимозависимости*, содержащий следующие утверждения:

> «Для эффективного цифрового сотрудничества необходимо укрепление многостороннего подхода, несмотря на существующие трудности. Также необходимо, чтобы многосторонний подход дополнялся принципом множества заинтересованных сторон — сотрудничество, в котором задействованы не только правительства, но гораздо более широкий спектр других заинтересованных сторон, таких как гражданское общество, академические круги, специалисты в области технологий и частный сектор» [25].

Хотя идея многостороннего подхода доказала свою продуктивность, она не пользуется единодушной поддержкой. До сих пор распространенным является мнение, что обеспечение международной безопасности и стабильности в подавляющем большинстве случаев является обязанностью государственных структур. Такой взгляд на безопасность является более традиционным и проистекает из представления о том, что государства несут ответственность за защиту своих граждан от нападений с применением силы. Эта идея отражена в обязанностях Совета Безопасности ООН, закрепленных в статье 24 Устава ООН [26]. Эта позиция также опирается на предыдущий опыт, поскольку в физическом мире правительства не только пользовались монополией на законное применение силы, но и контролировали боевые средства вооружения (например, самолеты, танки), использовавшиеся для нападения и обороны.

Однако на практике киберпространство является как результатом деятельности, так и полем конкуренции преимущественно негосударственных субъектов. Хотя правительственные органы занимают особое положение в контексте обеспечения безопасности собственных граждан, в киберпространстве они уже не выступают в такой роли. Даже если правительства *де-юре* сохраняют за собой монополию на легитимное применение силы в киберпространстве, в этой сфере у них больше нет фактической монополии на нападение и оборону и они не в состоянии предотвратить распространение и применение мощного кибероружия. Напротив, все более важную роль в защите киберпространства, включая внедрение соответствующих стандартов, начинают играть технические специалисты, гражданское общество и отдельные лица. Поэтому только многосторонний подход позволит обеспечить максимальную эффективность и создание обоснованных правил и правовых норм, помогающих поддерживать стабильность киберпространства и избежать нежелательных последствий.

Не менее важно и то, что, даже если государства захотят действовать самостоятельно, они не смогут этого добиться. Участие негосударственных субъектов в вопросах, влияющих на стабильность киберпространства, неизбежно. Например, критически важные протоколы и сервисы могут находиться в зоне ответственности различных представителей частного сектора и технического сообщества. Только такие лица будут в состоянии обеспечивать безопасность государственных структур, использующих их коммерческие продукты и продукты с открытым исходным кодом. Кроме того, даже расследование нападений и определение виновных — традиционная функция и политическая прерогатива правительств — уже перестали быть их исключительной компетенцией и ответственностью. Некоторые примечательные случаи кибератак, осуществленных при поддержке государственных структур, были выявлены и преданы гласности неправительственными организациями. Таким образом, даже если государство играет особую роль при нападении в киберпространстве и дальнейших действиях (включая деятельность правоохранительных органов и/или принятие мер дипломатического или иного характера), у него нет монополии на проведение расследований и установление ответственности. В равной степени правительственные органы не могут эффективно помешать деятельности негосударственных субъектов. В результате разработка успешных правил и правовых норм, регламентирующих действия в киберпространстве, равно как и обеспечение их соблюдения, требует участия и ответственности всех заинтересованных сторон, а правительства должны направить свои усилия на создание механизмов, которые обеспечат эффективное вовлечение в эту деятельность частного сектора, технических специалистов, ученых и других представителей гражданского общества. Именно к этому призывают многие правительства.

25 *Век цифровой взаимозависимости*, стр. 2: https://digitalcooperation.org/wp-content/uploads/2019/06/HLP-on-Digital-Cooperation-Report-Executive-Summary-RU.pdf.

26 Устав Организации Объединенных Наций, глава V. Совет Безопасности, справочник о деятельности органов Организации Объединенных Наций: https://www.un.org/ru/sections/un-charter/chapter-v/index.html.

5. ПРИНЦИПЫ

Нормативное поведение определяется ценностями. Поэтому отправной точкой должно стать провозглашение этих ценностей, независимо от того, относятся ли они к индивидуальной ответственности, ответственности государства или фундаментальным правам человека. В самом деле различия в ценностях могут затруднить достижение консенсуса, а также породить различия в толковании и реализации международных соглашений на уровне стран или регионов. Это не значит, что без согласования принципов прогресс невозможен. Иногда стороны договариваются о взаимоприемлемых правилах поведения даже в случае, когда их движущие мотивы отличаются. Однако общие принципы и взаимозависимость могут способствовать укреплению взаимных обязательств и снизить риск возникновения разногласий или конфликтов в будущем. Поэтому важно, чтобы стороны открыто обсуждали принципы высокого уровня, из которых они исходят и на основе которых формируются правовые нормы.

В обеспечении стабильности киберпространства решающую роль играют следующие четыре принципа.

1. **Ответственность:** каждый участник процесса несет ответственность за сохранение стабильности киберпространства.
2. **Дисциплина:** государственные и негосударственные субъекты не должны предпринимать действия, которые ставят стабильность киберпространства под угрозу.
3. **Необходимое вмешательство:** государственные и негосударственные субъекты должны принимать разумные и надлежащие меры для обеспечения стабильности киберпространства.
4. **Уважение прав человека:** усилия по обеспечению стабильности киберпространства не должны нарушать права человека и верховенство закона.

A. Принцип ответственности

Первый принцип связан с децентрализованной и распределенной структурой киберпространства. Он подтверждает необходимость многостороннего подхода к обеспечению стабильности киберпространства и, в частности, распространяет понятие «заинтересованные стороны» на каждого человека. Все из нас без исключения несут личную и/или профессиональную ответственность за обеспечение стабильности киберпространства. Наряду с очевидной ролью лиц, отвечающих за государственную киберполитику, и специалистов, управляющих облачными сервисами, каждый человек, так или иначе вовлеченный в киберпространство, должен предпринимать разумные усилия для защиты своих устройств от взлома и возможного использования для атак. Даже люди, не использующие подключение к Интернету, могут зависеть от его возможностей для получения товаров и услуг, и они также заинтересованы в том, чтобы в их сообществах проводилась надлежащая политика в отношении киберпространства.

B. Принцип дисциплины

Второй принцип предусматривает общее требование к дисциплине лиц, вовлеченных в киберпространство. Применительно к государствам это согласуется с резолюциями Генеральной Ассамблеи ООН от 2018 г. об ответственном поведении государств в киберпространстве [27] и докладом ГПЭ ООН от 2015 г., в котором отмечается следующее: «В соответствии с целями Устава Организации Объединенных Наций, в том числе касающимися поддержания международного мира и безопасности, государства должны сотрудничать в разработке и осуществлении мер по... предупреждению совершения действий в сфере ИКТ, признанных вредоносными или способных создать угрозу международному миру и безопасности» [28]. Но это требование касается не только правительственных органов, поскольку негосударственные субъекты также могут осуществлять ответные атаки на злоумышленников и подобные действия также могут подорвать стабильность киберпространства.

27 Резолюция Генеральной Ассамблеи ООН 73/27 *Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности*, A/RES/73/27, 5 декабря 2018 г.: https://undocs.org/ru/A/RES/73/27; и Резолюция Генеральной Ассамблеи ООН 73/266: https://undocs.org/ru/A/RES/73/266.

28 Доклад ГПЭ ООН 2015, стр. 10, п. 13 (a): https://undocs.org/ru/A/70/174.

C. Принцип необходимого вмешательства

Третий принцип содержит общее требование предпринимать продуктивные действия для поддержания стабильности киберпространства. При совершении таких действий государства должны позаботиться о том, чтобы не допустить непреднамеренной эскалации напряженности или нарастания нестабильности. Это согласуется с приведенным в докладе ГПЭ ООН от 2015 г. обязательством государств «...сотрудничать в разработке и осуществлении мер по укреплению стабильности и безопасности в использовании ИКТ»[29]. И вновь речь идет не только о государствах, поскольку частные компании и отдельные лица также могут предпринимать коллективные действия, направленные на обеспечение стабильности киберпространства. Например, компании могут сотрудничать в целях нейтрализации киберугроз, а отдельные лица должны следовать полезным рекомендациям, например своевременно обновлять ПО и устанавливать исправления или применять многофакторную аутентификацию для того, чтобы снизить риск проникновения в свои компьютеры ботнетов и последующего их использования для проведения широкомасштабных атак, угрожающих стабильности киберпространства.

D. Принцип уважения прав человека

Четвертый принцип признает значение защиты прав человека как важного элемента стабильности киберпространства. По мере того как в жизни людей расширяется роль информационно-коммуникационных технологий, угрозы, связанные с их доступностью или защищенностью, становятся все более разрушительными для человеческой деятельности. Поэтому крайне важно, чтобы в процессе отстаивания своих национальных стратегических интересов в киберпространстве государства уделяли должное внимание их воздействию на отдельных лиц, в частности на соблюдение прав человека. Точно так же негосударственные субъекты должны учитывать и минимизировать риски нарушения прав отдельных лиц в Интернете и за его пределами, связанные с деятельностью таких субъектов. Как минимум следование упомянутому выше принципу требует, чтобы при осуществлении деятельности в киберпространстве государства придерживались своих международно-правовых обязательств в области прав человека.

Общепризнанные права человека закреплены во Всеобщей декларации прав человека [30]. Кроме того, существует множество международных соглашений, которые декларируют особые права человека и накладывают на государства — участники таких соглашений определенные правовые обязательства. Применимость международных норм в области прав человека в контексте киберпространства неоднократно прямо подтверждалась Генеральной Ассамблеей Организации Объединенных Наций [31], Советом ООН по правам человека (СПЧ) [32], а также докладами ГПЭ ООН от 2013 и 2015 гг. [33] Защита прав пользователей и уверенность пользователей в соблюдении своих прав имеют решающее значение для обеспечения стабильности киберпространства.

Мы отмечаем, что эти четыре принципа не претендуют на полноту и не охватывают все аспекты политики в отношении киберпространства. Отметим, что многие организации разработали собственные комплексные принципы, также охватывающие широкий круг вопросов. Существуют и другие организации, которые занимаются вопросами, связанными с управлением Интернетом и правами человека в киберпространстве (включая неприкосновенность частной жизни, свободу выражения мнений и свободу объединений). Наша цель — добиться широкого признания принципов, поддерживающих стабильность киберпространства, особенно в эпоху беспрецедентной и изощренной враждебной деятельности, когда правила могут быть нечеткими или, даже если они четко определены, могут не соблюдаться и не обеспечиваться.

29 Там же.

30 Резолюция Генеральной Ассамблеи ООН 217 A (III) *Всеобщая декларация прав человека*, 10 декабря 1948 г.: https://www.un.org/ru/universal-declaration-human-rights/.

31 См. Резолюцию Генеральной Ассамблеи ООН 68/167 *Право на неприкосновенность личной жизни в цифровой век*, A/RES/68/167 (18 декабря 2013 года), https://undocs.org/ru/A/RES/68/167; и Резолюцию Генеральной Ассамблеи ООН 69/166 *Право на неприкосновенность личной жизни в эпоху цифровых технологий*, A/RES/69/166, 18 декабря 2014 г.: https://undocs.org/ru/A/RES/69/166.

32 Совет ООН по правам человека, *Поощрение, защита и осуществление прав человека в Интернете*, A/HRC/20/L.13, 29 июня 2012 г.: https://undocs.org/ru/A/HRC/20/L.13.

33 Доклад ГПЭ ООН от 2013 г.: https://undocs.org/ru/A/68/98; доклад ГПЭ ООН от 2015 г.: https://undocs.org/ru/A/70/174.

6. НОРМЫ

Хотя принципы являются ключевым отправным пунктом для выработки правил и осуществления общей стратегии, их высокий уровень абстракции требует дополнить их более подробными соглашениями, определяющими приемлемое поведение. Это означает, что принципы должны быть дополнены правовыми нормами. Нормы представляют собой социальные модели ожидаемого и адекватного поведения [34]. Невозможно обсуждать нормы, не ссылаясь на работу других организаций, особенно ГПЭ ООН и ее доклад за 2015 г. [35]. ГПЭ ООН признала, что «...с учетом уникальных особенностей ИКТ со временем может возникнуть необходимость в разработке дополнительных норм» [36] и что мандат Глобальной комиссии по стабильности киберпространства заключается в том, чтобы «...разработать предложения в области правил и правовых норм, необходимых для укрепления международной безопасности и стабильности». Чтобы использовать результаты уже проделанной работы и выявить, где могут потребоваться дополнительные нормы, важно начать с норм, принятых в 2015 г., которые в полном объеме приводятся в приложении А.

В докладе ГПЭ ООН от 2015 г., наряду с другими задачами, было поставлено требование выяснить, в каких случаях может потребоваться разработка дополнительных норм, которые бы учитывали сложные и уникальные особенности ИКТ [37]. С тех пор продукты и сервисы ИКТ, равно как и способы их неправомерного использования, продолжают неизменно меняться. Для решения этой задачи Комиссия сосредоточилась на восполнении пробелов в имеющемся комплексе норм, привнесении в обсуждение норм технической специфики и решении вопросов, связанных с их внедрением. Например, в целях восполнения пробелов в законах Комиссия поддержала норму по защите ядра Интернета [38] и норму по защите электоральных систем [39]. Аналогичным образом, если норма ГПЭ ООН ссылается на «целостность каналов поставки» [40], то в норме Комиссии говорится более конкретно о видах атак на каналы поставки, с которыми необходимо бороться [41].

34 https://en.oxforddictionaries.com/definition/norm.

35 Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, 2015, https://undocs.org/ru/A/70/174

36 Там же, с. 8, п. 15

37 Там же, с. 7, п. 11

38 Глобальная комиссия по стабильности киберпространства (GCSC), *"Призыв к защите публичного ядра Интернета" (Call to Protect the Public Core of the Internet)* (Нью-Дели, ноябрь 2017), https://cyberstability.org/wp-content/uploads/2018/07/call-to-protect-the-public-core-of-the-internet.pdf. Голландский исследователь Деннис Брудерс является давним сторонником идеи определения общедоступного ядра Интернета для обеспечения его особой защиты. См. Деннис Брудерс (Dennis Broeders), *"Публичное ядро Интернета" (The Public Core of the Internet:) "Международный план действий по управлению Интернетом" (An International Agenda for Internet Governance)* (Amsterdam: Amsterdam University Press, Amsterdam, 2015 (Амстердам), http://www.oapen.org/download?type=document&docid=610631.

39 Глобальная комиссия по стабильности киберпространства (GCSC), *Призыв к защите избирательной инфраструктуры (Call to Protect the Electoral Infrastructure)* (Братислава, май 2018), https://cyberstability.org/wp-content/uploads/2018/05/ GCSC-Call-to-Protect-Electoral-Infrastructure.pdf.

40 Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, 2015, с. 8, п. 13(i), «Государства должны принимать разумные меры для обеспечения целостности каналов поставки, чтобы конечные пользователи могли быть уверены в безопасности продуктов ИКТ. Государства должны стремиться предупреждать распространение злонамеренных программных и технических средств в сфере ИКТ и использование пагубных скрытых функций».

41 Глобальная комиссия по стабильности киберпространства (GCSC), *"Нормы при посредничестве Сингапура" (Norms Through Singapore)* (ноябрь 2018), https://cyberstabil-ity.org/wp-content/uploads/2019/04/singaporenew-digital.pdf. «Государственные и негосударственные субъекты не должны вмешиваться в разработку и производство продуктов и услуг или позволять подобное вмешательство, если это может существенно навредить стабильности киберпространства».

Другое существенное различие между нормами ГПЭ ООН и нормами, предлагаемыми Комиссией, заключается в том, что, по нашему мнению, обязанности должны быть возложены и на негосударственные субъекты, поскольку они должны соблюдать ограничения или предпринимать конструктивные действия для обеспечения стабильности киберпространства. Мы здесь не имеем в виду кибератаки со стороны преступников. Злоумышленников, деятельность которых не в состоянии предотвратить правительство, не сдержат и нормы. Но поскольку технологии меняются быстро, а законы — нет, то целесообразно точно определить, какое модели поведения негосударственных субъектов должны поощряться или пресекаться даже в отсутствие законов. Например, некоторые лица выступают за то, чтобы предоставить жертвам взлома право на «ответный удар». Даже в отсутствие законов, разрешающих или запрещающих подобное поведение, Комиссия считает его нецелесообразным по нескольким причинам, включая тот факт, что исходный злоумышленник может направить свою атаку через сторонние системы (например, через поставщика облачных услуг или больницу), поэтому ответный удар может поразить непричастных пользователей (например клиентов облака или пациентов). Кроме того, из-за таких нападений на непричастных лиц ответный удар может рассматриваться как эскалация или спровоцировать ее. Иными словами, из-за возникающих сложностей даже в отсутствие законов норма, ограничивающая деятельность субъектов частного сектора, может влиять на их поведение и тем самым приносить пользу.

A. Нормы, предлагаемые Комиссией

С учетом вышеизложенного Глобальная комиссия по стабильности киберпространства предлагает внедрить следующие нормы.

1. Государственные и негосударственные субъекты не должны вести или сознательно допускать деятельность, которая преднамеренно наносит существенный ущерб общедоступности или целостности ядра Интернета и, как следствие, стабильности киберпространства.

2. Государственные и негосударственные субъекты не должны проводить, поддерживать или допускать кибероперации, направленные на нарушение нормальной работы технической инфраструктуры, необходимой для проведения выборов, референдумов или плебисцитов.

3. Государственные и негосударственные субъекты не должны вмешиваться или допускать вмешательство в разработку и производство товаров и услуг, если такое вмешательство может существенно нарушить стабильность киберпространства.

4. Государственные и негосударственные субъекты не должны присваивать общие публичные ресурсы ИКТ для использования их в качестве ботнетов или в аналогичных целях.

5. Государства должны создать прозрачные с процедурной точки зрения методики, позволяющие оценивать, когда следует (и следует ли) сообщать общественности об уязвимостях или недостатках информационных систем или технологий. По умолчанию подобные сведения всегда следует обнародовать.

6. Разработчики и производители продуктов и услуг, от которых зависит стабильность киберпространства, должны (1) отдавать приоритет безопасности и стабильности; (2) предпринимать разумные шаги для обеспечения того, чтобы их продукты или услуги не подвергались значительной уязвимости; и (3) своевременно принимать меры в отношении уязвимостей, которые обнаруживаются впоследствии, и обеспечивать прозрачность этих мер. Все участники обязаны обмениваться информацией об уязвимостях, чтобы помочь предотвратить или смягчить злонамеренную киберактивность.

7. Государства должны принимать соответствующие меры, в том числе утверждать законы и правовые нормы, которые будут гарантировать элементарную гигиену киберпространства.

8. Негосударственные субъекты не должны участвовать в атакующих кибероперациях, а государственные структуры должны предотвращать подобные действия и реагировать в тех случаях, если они совершаются.

Стоит отметить, что выбор подходящего языка для выражения этих норм может оказаться непростой задачей. Если нормы будут сформулированы слишком жестко, не оставляя места толкованию, это может затруднить достижение консенсуса и привести к большим пробелам в сфере охвата. С другой стороны, слишком размытые нормы не обеспечат надлежащее руководство в вопросах поведения и не сформируют четкие ожидания от конкретных групп субъектов. Таким образом, следует стремиться к золотой середине, разрабатывая при необходимости дополнительные нормы, чтобы охватить все формы нежелательного поведения. В качестве примера можно привести нормы, принятые созданной ООН Группой правительственных экспертов (GGE) в 2015 году, которые защищали критически важные инфраструктуры, но из которых было непонятно, относится ли к подобным инфраструктурам общедоступное ядро Интернета, ведь для многих критически важные инфраструктуры — это инструменты и услуги (например, в сфере электроэнергии, коммуникаций и банковских услуг). [42] Кроме того, GGE ООН не упомянула избирательные системы, вопрос которых стал еще более актуальным после 2015 года. [43] В нормах некоторых стран дается отсылка на избирательные системы (то есть, некоторые государства начали расценивать избирательные системы как критически важную инфраструктуру, включая их тем самым в диапазон охвата соответствующих норм), [44] но не все страны могут захотеть последовать этому примеру. Таким образом, пусть киберпространство и является глобальным, нормы его защиты не всегда могут быть такими же. Для урегулирования вопросов толкования норм GCSC комиссия решила предоставить справочный текст для каждой из изложенных выше норм (см. Приложение B).

Наконец, важно понимать, что нормы поведения в киберпространстве не могут быть статичны. Нормы GCSC отражают лишь один момент в непрерывно меняющемся мире технологий. Государственные и негосударственные субъекты должны быть готовы к необходимости разрабатывать новые нормы по мере развития технологий и изменений нашего понимания о том, что заключают в себе существующие технологии.

Важно понимать, что для обеспечения эффективности норм — будь то нормы GGE ООН, нормы GCSC или другие предложения — необходимо внедрить и соблюдать их, призывая к ответу за их нарушение. Сейчас мы занимаемся урегулированием этих аспектов, прежде чем переходить к следующему — как объединить разобщенные и распределенные по всему миру негосударственные субъекты для сотрудничества с властями в области разработки практических решений проблем, связанных с киберстабильностью.

B. Принятие норм

Для того, чтобы норма была эффективной, она должна быть принята повсеместно. Подобное принятие, даже со стороны субъектов, которые могут расцениваться как потенциальные нарушители нормы, укрепляет легитимность действий, обличающих нарушения норм, а также уместных коллективных действий, предпринимаемых в ответ на такие нарушения. Оптимальным вариантом будет повсеместное принятие норм, но и менее масштабные альянсы государств-единомышленников или других структур, согласующих и принимающих конкретные нормы, также немаловажны.

42 Критически важная инфраструктура определяется как включающая в себя «системы и активы, как физические, так и виртуальные, являющиеся настолько важными, что их неисправность или уничтожение окажут подрывное воздействие на общую безопасность, национальную экономическую безопасность, на общественное здравоохранение и безопасность или на несколько этих сфер сразу. *Закон 2001 года о защите важнейших объектов инфраструктуры (Critical Infrastructures Protection Act of 2001)*, ст. 42 Кодекса США § 5195c(e), (2001). Кроме того, она была определена как «активы или системы, которые жизненно важны для поддержания социальных функций, здравоохранения, безопасности, а также экономического и социального благополучия народа». Совет Европейского союза, *Директива Совета ЕС 2008/114/ЕС от 8 декабря 2008г. по выявлению и обозначению европейских (on the Identification and Designation of European)*
важнейших объектов инфраструктуры и оценки необходимости улучшения их защиты (Critical Infrastructures and the Assessment of the Need to Improve Their Protection), Официальный журнал Европейского союза (Official Journal of the European Union), (8 декабря 2008), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114.

43 Эрик Браттберг и Тим Маурер (Erik Brattberg and Tim Maurer), *"Вмешательство России в выборы" (Russian Election Interference): Европейский подсчет фейковых новостей и кибератак (Europe's Counter to Fake News and Cyber Attacks),* Фонд Карнеги "За международный мир" (23 мая 2018), https://carnegieendowment.org/2018/05/23/russian-election-int europes-counter-to-fake-news-and-cyber-attacks-pub-76435. См. также Майкл Макфол изд. (Michael McFaul, ed.), *"Обеспечение безопасности американских выборов" (Securing American Elections),* Стэнфордский центр киберполитики (июнь 2019), https://cyber.fsi.stanford. edu/securing-our-cyber-future.

44 См., например, Министерство внутренней безопасности США, "Заявление секретаря Джея Джонсона об определении избирательной инфраструктуры в качестве участка важнейшей инфраструктуры", 2017 (U.S. Department of Homeland Security, Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector, 2017), https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

Для поддержания таких альянсов GCSC предлагает гибкий и всеобъемлющий подход, позволяющий государствам и другим заинтересованным сторонам принимать одни нормы, отклоняя при этом другие или воздерживаясь от принятия решения по ним. Такой подход не только вносит ясность, выделяя конкретные области, по которым удалось или не удалось прийти к согласию, но и позволяет принять, усовершенствовать и внедрить определенные нормы, даже если для оценки других требуется больше времени. Как бы там ни было, повсеместного принятия норм невозможно достичь в одночасье.

Кроме того, в продвижении принятия норм есть свои уникальные подводные камни и проблемы практического характера. Уникальная проблема заключается в том, что мы имеем дело с относительно новыми формами дестабилизирующего поведения. В свете определения нормы как «чего-то общепринятого, типичного или стандартного» [45] разработка норм в отношении будущего поведения становится интересной задачей. Если все уже привыкли вести себя каким-то образом, то письменная норма просто закрепляет существующую практику. Тем не менее, если «стандартное поведение» еще не выработано, то разработка нормы превращается в попытку призыва к определенному общепринятому поведению в будущем, даже если на данный момент такого общепринятого поведения еще не существует. Простого заявления о том, что какая-то форма поведения является желательной, недостаточно для того, чтобы сделать ее нормой, поэтому принятие норм необходимо продвигать.

Кроме того, необходимо обеспечить более широкую информированность о предлагаемых нормах для субъектов, которые способны внедрить их, а также для тех, кого эти нормы призваны защищать. Несмотря на значительную активность со стороны ООН и проведение других форумов, принятие норм все еще находится на относительно зачаточном этапе — требуется приложить немало усилий для продвижения и обеспечения принятия предлагаемых норм, особенно в некоторых странах. Именно поэтому наращивание потенциала в этой сфере имеет такое большое значение; организации с более мощным потенциалом с большей вероятностью смогут эффективно поддержать принятие норм, а привлечение дополнительных сторонников — это фундамент любой глобальной нормативной структуры. Кроме того, необходимо привлекать субъектов, которых эти нормы призваны защищать, поскольку они могут не знать о возможных последствиях принятия этих норм. Например, по всей видимости, компьютерные группы реагирования на чрезвычайные ситуации (CSIRT/CERT) при GGE ООН не очень хорошо осведомлены о норме, запрещающей государствам атаковать национальные CSIRT и использовать их исключительно в оборонных целях. Как будет изложено ниже, защищаемым субъектам будет часто отводиться роль в процессах внедрения и привлечения к ответственности за нарушения (равно как и в разработке предлагаемой нормы), но они не смогут справиться со своей ролью без осознания и понимания норм, выдвигаемых государственными и негосударственными субъектами. Очевидно, что государства и международные организации должны активнее работать над привлечением тех сообществ, которым предлагаемые нормы призваны помогать.

45 См. https://www.lexico.com/en/definition/norm.

C. Внедрение норм

После принятия нормы государственные и негосударственные субъекты должны предпринять конкретные меры для ее внедрения. Очевидно, что между нынешними процессами ООН (со стороны OEWG и GGE) и региональными усилиями постепенно намечается консенсус о том, что внедрение норм является приоритетом. [46] Для кого-то внедрение связано с принятием нормы, с усилиями по наращиванию ее потенциала и формированием мер, направленных на укрепление доверия, либо с достижением более детального консенсуса в отношении значения согласованной нормы. [47] Разумеется, эти меры — важные предварительные условия для внедрения норм, но сами по себе они не являются инструментами для их внедрения. Например, нарастить потенциал для того, чтобы государства могли обеспечить собственную безопасность и достаточную пропускную способность для выхода на международный уровень с точки зрения киберпространства, можно и без принятия или внедрения норм. Аналогичным образом, хотя меры по укреплению доверия могут помочь в поддержании стабильности киберпространства, способствуя международному обмену мнениями по поводу кибердоктрины, устанавливая оперативные каналы связи для общения между национальными экспертами в сфере киберпространства и поощряя обмен лучшими практиками и стандартами безопасности, их тоже можно осуществлять без внедрения норм. Внедрение нормы, напротив, предполагает конкретные шаги для придания ей обязывающей силы. На уровне страны такие шаги могут подразумевать внедрение предложенных норм в государственную политику, законодательство и военную доктрину. На международном уровне сюда может относиться цитирование положений нормы при вменении в вину атак или принятие дипломатических мер. Подобная

46 Резолюция Генеральной Ассамблеи 73/266, с. 3, п. 1(b), https://undocs.org/ru/A/RES/73/266; Резолюция Генеральной Ассамблеи 73/27, с. 5, п. 5, https://undocs.org/ru/A/RES/73/27. Организация по безопасности и сотрудничеству в Европе (ОБСЕ), *Вступительное слово Генерального секретаря Томаса Гремингера (Opening remarks by Secretary General Thomas Greminger)*, 2019 Председательство на конференции ОБСЕ по кибернетической / ИКТ-безопасности, Братислава, 2019 (Chairmanship OSCE-wide cyber/ICT security conference, Bratislava, 2019). «Региональные организации... могут стать инкубаторами для новых идей и практических усилий, связанных с мерами по укреплению доверия, а также инструментом внедрения принятых на международном уровне соглашений, таких как отчет GGE. Таким образом, региональные организации — это и инкубаторы, и механизмы внедрения».

47 Генеральная Ассамблея просит 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, указывая *в том числе,* «усилия, предпринимаемые на национальном уровне для укрепления информационной безопасности и содействия международному сотрудничеству в этой области» и «возможные меры, которые могли бы быть приняты международным сообществом для укрепления информационной безопасности на глобальном уровне». См. Доклад Генерального секретаря ООН 74/120, https://undocs.org/ru/A/74/120. Подробнее о взглядах конкретных стран-участниц см. на https://www.un.org/disarmament/ru/достижения-в-сфере-информатизации-и-т/.

практическая реализация нормы также помогает дать ей более точное определение.

D. Привлечение к ответственности

После принятия и внедрения норм необходимо установить процедуру привлечения к ответственности за их нарушение. Эта задача сопряжена со сложными вопросами вменения в вину и возражения против нее, которые не так просто согласовать, когда речь идет о кибератаках.

Чтобы утверждать, что государственный или негосударственный субъект поступил неправомерно, необходимо иметь достоверное обоснование. Для формирования такого обоснования требуется собрать и проанализировать улики — с технической и процессуальной точек зрения с этой задачей можно начать работать уже сейчас, чтобы усовершенствовать качество и своевременность предоставления обоснования. Говоря более конкретно, наличие общепринятых протоколов для сбора и анализа улик, как и в других технических дисциплинах играет важную роль для повышения качества расследований. Таким образом, стандартизация методов расследования имеет большое значение, поскольку позволяет снизить долю сомнений в достоверности улик, даже если вменение в вину реализуется с учетом специфики конкретного дела. Процесс вменения в вину можно улучшить не только технически. Существует множество способов, позволяющих смягчить бюрократический аспект, связанный с принятием решений о вменении в вину и их обнародованием, когда это уместно. Зачастую, значительная задержка между событием и заявлением об ответственности объясняется, во многом, нечеткими или тяжеловесными процедурами принятия подобных решений на государственном уровне и становится еще больше, когда в этом процессе участвуют несколько стран. Разработка и реализация процессов для рассмотрения нарушений на государственном и международном уровнях, а также укрепление информационного обмена между странами могут заметно повысить своевременность и эффективность рассмотрения исков и способствовать принятию соответствующих мер.

Даже если улики указывают на определенного субъекта, следующий шаг (вменение в вину) может оказаться не так прост. Раньше некоторые государственные и негосударственные субъекты могли принять решение о том, что вменение в вину невозможно или требует абсолютного доказательства. Тем не менее, сейчас мы понимаем, что абсолютное доказательство не является необходимостью и что, хотя процесс вменения в вину нарушения может быть не прост, он все же не настолько непреодолим, как полагают некоторые. В контексте государства, вменение в вину — как в кибер-, так и в физическом мире — часто является политическим актом, а при отсутствии конкретного согласованного стандарта доказательства страны по-прежнему стремятся не делать сомнительных утверждений, чтобы не потерять доверие. Вкратце, решение о вменении в вину должно выглядеть убедительным в глазах других стран и общественности.

Даже если потерпевшая сторона удовлетворена возложением на определенного субъекта ответственности (и решение о вменение в вину было принято на международном уровне), реально привлечь этого субъекта к ответственности может быть сложно, что несколько преуменьшает ценность норм. В конечном итоге, при отсутствии негативных последствий для нарушителей принятых норм эти нормы становятся лишь немногим более значимыми, чем слова на бумаге, и вряд ли остановят желание заниматься дестабилизирующей деятельностью.

Привлечение к ответственности за кибератаки негосударственными субъектами — процесс относительно прямой и реализуемый, в основном, за счет возложения гражданской или уголовной ответственности в рамках внутреннего права конкретной страны. Конечно, этот процесс тоже не лишен своих трудностей, поскольку международный характер многих кибератак и технические сложности при сборе улик могут чинить препятствия осуществлению акта государственной власти. Тем не менее, концепция плана дальнейших действий понятна: упростить процессы международной правоохранительной практики и стремиться к обнаружению и наказанию киберпреступников.

Привлечение целых стран к ответственности за нарушение норм — задача посложнее, [48] поскольку реагирование на атаку в киберпространстве очень сильно зависит от контекста. При принятии решения о необходимости привлечения к ответственности государственные и негосударственные субъекты будут учитывать разные факторы; например, государство, реагирующее на нарушение норм, будет думать о политических последствиях, а частная компания — о последствиях для бизнеса и репутации. В отношении способов реагирования на нарушение норм ряд доступных государству мер уходит в бесконечность — реакция может быть незначительной (например, частная жалоба), существенной (например, экономические санкции) или радикальной (например, хорошо заметные динамические меры). Невозможно подогнать все меры под один масштаб, но очевидно, что нарушение норм и положений международного права должно иметь значительные последствия. Поскольку прошлые попытки принуждения к соблюдению норм не имели большого успеха, необходимо разработать более эффективные и своевременные меры с расчетом на то, что эти меры должны свести к минимуму дальнейшую нестабильность.

Негосударственные субъекты тоже работают над способами привлечения нарушителей норм к ответственности за их действия. Например, в GFCE [49] представители власти, гражданского общества и частного сектора сообща помогают координировать усилия для наращивания правового потенциала, что является обязательным предварительным условием для принятия и внедрения норм и привлечения к ответственности за их нарушение. Кроме того, частный сектор взял на себя расширенную роль в отношении привлечения к ответственности за атаки, используя и собственную, и общественную информацию для вменения субъектам в вину

48 Государства могут нести ответственность за проводимые, направляемые или разрешаемые ими операции в киберпространстве. Принцип должной осмотрительности также может быть полезен для определения уровня заботы в отношении киберпространства со стороны государств. Джоанна Кулеса (Joanna Kulesza), *"Правовой анализ в международном праве" (Due Diligence in International Law)*, (Leiden: Brill Nijhoff, 2016, https://doi.org/10.1163/9789004325197. См. также, *Статьи об ответственности государств за международно-противоправные деяния (Articles on Responsibility of States for Internationally Wrongful Acts)*, приняты Комиссией по международному праву на ее пятьдесят третьей сессии в 2001 году, связаны с резолюцией 56/83 Генеральной Ассамблеи от 12 декабря 2001 года и исправлены в документе A/56/49 (Vol I) / Corr4, статьи 4 и 11, https://legal.un.org/avl/pdf/ha/rsiwa/rsiwa_r.pdf.

49 Global Forum on Cyber Expertise, https://www.thegfce.com/.

причиненного ими ущерба и описания этого ущерба. Наконец, некоторые структуры частного сектора предложили или уже запустили определенные инициативы, такие как «Институт кибермира»(CyberPeace Institute) [50], предназначенные для более систематического и потенциально более масштабного отслеживания и освещения крупных событий в киберсфере.

Негосударственные субъекты должны взять на себя более активную роль в привлечении нарушителей норм к ответственности. Сама по себе идея участия частного сектора в исполнении норм не нова: например, в 1977 году, в период борьбы с апартеидом в ЮАР, компания General Motors поддержала ряд широко применимых принципов ведения бизнеса (и воздержания от ведения бизнеса) в стране, в результате чего свыше 125 зарубежных компаний вывели свои инвестиции. [51] Из более недавнего и более символического — многие компании (и правительства) отреагировали на убийство репортера от оппозиции Джамаля Хашогги из Саудовской Аравии, бойкотировав инициативу «Инвестиции будущего» в знак своего неодобрения. [52] Подобные виды усилий заслуживают дальнейшего изучения.

E. Сообщества по интересам

Привлечение многих заинтересованных сторон к процессам принятия, внедрения норм и вменения в вину их нарушения — бесспорно, критически важный аспект, но использовать энергию и потенциал таких многогранных групп не так просто. Государства часто используют термин «страны-единомышленницы» в отношении группы стран со схожими взглядами, но нет аналогичного термина, который бы подразумевал группу стран, частных компаний, некоммерческих организаций (включая организации по стандартизации), гражданское общество и физических лиц, разделяющих взгляды по какому-либо вопросу. Это важный момент, поскольку предложенные Глобальной комиссией по стабильности киберпространства (GCSC) и Группой правительственных экспертов (GGE) при ООН нормы могут затрагивать разные структуры, то есть какие-то организации и члены общества могут быть больше остальных заинтересованы в поддержке определенных норм. Поскольку правительства, частный сектор, техническое сообщество, научно-образовательное сообщество и гражданское общество не являются монолитными структурами, следует подумать о том, как сформировать согласованный, а не сконцентрированный потенциал, чтобы привлечь разные сообщества к решению связанных с нормами вопросов. [53] Создание сообществ по интересам позволяет тем, у кого есть опыт и знания в отношении конкретных норм, работать над их развитием и внедрением. Например, компьютерные группы реагирования на чрезвычайные ситуации (CSIRT/CERT) могут особо заинтересоваться внедрением и отслеживанием соблюдения нормы Группы правительственных экспертов (GGE) при ООН, нацеленной на защиту сообществ. Те же, кто отвечает за избирательные системы, могут больше заинтересоваться нормой GCSC об избирательных системах.

Аналогичным образом, интернет-сообщество может помочь в развитии, внедрении и отслеживании соблюдения предложенной Комиссией нормы о защите публичного ядра интернета, а разработчиков может больше всего заинтересовать норма, связанная с вмешательством в продукты.

Формирование сообщества по интересам может быть направленным или ситуативным, осуществляемым «снизу-вверх» процессом. Тот факт, что сами члены комиссии могут сформировать сообщество, не подразумевает, что его развитие и успех следует предоставить воле случая. Напротив, важно сосредоточиться на тех аспектах, которые делают сообщество успешным: (1) общие принципы; (2) нацеленность на решение вопросов; (3) компетенция в предметной области; (4) финансовая и административная поддержка; и (5) прозрачность процессов. По сути, можно разработать оптимальный шаблон для создания и внедрения сообществ, что позволит использовать одинаковую модель сообщества в разных процессах установления норм. Это поможет согласовать разные рабочие потоки для обеспечения эффективности и фокусирования на задачах, а также использовать лучшие практики для принятия и внедрения норм и привлечения к ответственности за их нарушение.

50 CyberPeace Institute, https://cyberpeaceinstitute.org/.

51 См. в целом, "Принципы Салливана" (“Sullivan Principles”), Wikipedia, 12 августа 2018, https://en.wikipedia.org/wiki/Sullivan_principles.

52 См. "Бойкот Запада инвестиционной инициативы будущего 2018"(“Western boycott of Future Investment Initiative 2018”), *Royal News*, 16 октября 2018, https://en.royanews.tv/ news/15500/2018-10-16.

53 См. в целом *"Эпоха цифровой взаимозависимости" (The Age of Digital Interdependence)*, https:// digitalcooperation.org/wp-content/uploads/2019/06/DigitalCo-operation-report-for-web.pdf.

7. РЕКОМЕНДАЦИИ

Шесть наших рекомендаций для обеспечения стабильности киберпространства происходят из наших принципов в отношении ответственности, сдерживания, требования к действию и уважения прав человека. Поскольку ответственность за обеспечение стабильности киберпространства несет каждый, и с учетом важности привлечения многих заинтересованных сторон наши рекомендации также нацелены на использование потенциала государственных и негосударственных субъектов, отчасти с помощью сообществ по интересам. Вкратце, мы концентрируемся на том, что *необходимо* сделать и каким образом это *возможно* осуществить.

1. **Государственные и негосударственные субъекты должны принять и внедрить нормы, способствующие повышению стабильности киберпространства, путем поддержки сдерживающих и поощрительных мер.** Государственные субъекты, которые уже приняли нормы, должны дать более четкие определения используемым в них терминам. Для этого требуются дальнейшие переговоры и практический опыт внедрения существующих норм. И государственные и негосударственные субъекты должны предоставить четкие доказательства принятия и внедрения норм с помощью публичных заявлений и перемен с политической и практической точки зрения.

2. **Государственные и негосударственные субъекты должны реагировать на нарушение норм в надлежащей манере и в соответствии с их обязанностями и ограничениями, следя за тем, чтобы нарушители испытывали предсказуемые и значимые последствия.** Разработка и внедрение норм не будут эффективными, если нарушители будут знать, что их поступки останутся безнаказанными. Таким образом, государственные и негосударственные субъекты должны наращивать внутренний потенциал для оценки нарушений и быстрого принятия решений о надлежащих индивидуальных и коллективных мерах, соответствующих принципу требования к действию.

3. **Государственные и негосударственные субъекты, включая международные организации, должны прилагать больше усилий для обучения сотрудников, наращивания потенциала и возможностей и продвижения общего понимания важности стабильности киберпространства, учитывая при этом разноплановые нужды разных сторон.** Наращивание потенциала и возможностей, наряду с укреплением понимания позволит повысить мировую компетентность в вопросах внедрения положений международного права, норм и других повышающих доверие мер, призванных повысить стабильность киберпространства при одновременном соблюдении прав человека. Все стороны должны использовать потенциал уже имеющихся организаций, включая многосторонний Глобальный форум по вопросам киберпространства (Global Forum on Cyber Expertise), направленных на наращивание возможностей, поскольку это является обязательным предварительным условием для принятия и внедрения норм, обеспечения их соблюдения путем привлечения к ответственности за нарушения, принятия других мер по укреплению стабильности и соблюдения прав человека.

4. **Государственные и негосударственные субъекты должны собирать, изучать и публиковать информацию о нарушениях норм и последствиях таких действий, а также делиться подобной информацией.** Хотя мир уже был свидетелем действий, которые расцениваются как нарушение норм, установленных ООН и предложенных GCSC, система отчетности остается в большей степени ситуативной, нежели комплексной. Организации — особенно те, которые не зависят от государственных или коммерческих интересов — должны систематически собирать и публиковать информацию о нарушениях норм и последствиях этих нарушений. Таким образом можно будет активировать реагирование государственных и негосударственных субъектов на нарушения норм и обеспечить более эффективное соблюдение норм.

5. **Государственные и негосударственные субъекты должны сформировать и поддерживать сообщества по интересам в целях обеспечения стабильности киберпространства.** Формирование и поддержка таких сообществ поможет гарантировать соблюдение всеми заинтересованными сторонами, включая государства, частный сектор, техническое сообщество, научно-образовательное сообщество и гражданское общество, своих обязанностей в отношении обеспечения

стабильности киберпространства. В числе прочего, эти сообщества могут сосредоточиться на таких аспектах, как толкование, принятие и внедрение норм кибербезопасности, изложенных в данном отчете и в других документах, а также изучать жизнеспособность стандартов в отношении критериев доказательности при привлечении к ответственности за нарушения и следить за тем, чтобы привлечение нарушителей к ответственности осуществлялось в своевременной и эффективной манере.

6. **GCSC рекомендует создать для решения вопросов стабильности постоянный механизм привлечения многих сторон, включая государства, частный сектор (в том числе, техническое сообщество) и гражданское общество, которые будут равнозначными участниками и консультантами в этих процессах.** Принцип ответственности гласит, что каждый субъект имеет свою роль в обеспечении стабильности киберпространства, а также поддерживает необходимость многостороннего подхода. В период с 2011 по 2017 гг. Глобальная конференция по киберпространству (GCCS) разработала единую платформу для подобного привлечения многих сторон, включив в процесс чиновников из министерств иностранных дел и министерств безопасности, на которых была возложена задача по обеспечению глобальной стабильности в других сферах. Кроме того, эта платформа стала отправной точкой для учреждения Глобального форума по вопросам киберпространства (Global Forum on Cyber Expertise), который является важной инициативой по наращиванию потенциала. Форум по управлению использованием Интернета (IGF) также предложил полезную платформу для многосторонних обсуждений. Если говорить о более недавних инициативах, следует упомянуть Paris Call, объединившую крупнейшее в истории многостороннее сообщество сторонников норм кибербезопасности. Все эти инициативы указывают на то, что сейчас самый подходящий момент для формирования глобального, инклюзивного и ориентированного на действие многостороннего общества, нацеленного на практическое внедрение норм кибербезопасности, изложенных в данном отчете и в других документах. Такой подход должен опираться на постоянную структуру для поддержки устойчивых и непрерывных усилий.

ПРИЛОЖЕНИЕ A: НОРМЫ, ПРИНЯТЫЕ ГРУППОЙ ПРАВИТЕЛЬСТВЕННЫХ ЭКСПЕРТОВ (GGE) ПРИ ООН[54]

a. в соответствии с целями Устава Организации Объединенных Наций, в том числе касающимися поддержания международного мира и безопасности, государства должны сотрудничать в разработке и осуществлении мер по укреплению стабильности и безопасности в использовании ИКТ и предупреждению совершения действий в сфере ИКТ, признанных вредоносными или способных создать угрозу международному миру и безопасности;

b. в случае инцидентов в сфере ИКТ государства должны изучить всю соответствующую информацию, в том числе более общий контекст события, проблемы присвоения ответственности в ИКТ-среде, а также характер и масштабы последствий;

c. государства не должны заведомо позволять использовать их территорию для совершения международно-противоправных деяний с использованием ИКТ;

d. государства должны рассмотреть вопрос о наилучших путях сотрудничества в целях обмена информацией, оказания взаимопомощи, преследования лиц, виновных в террористическом и преступном использовании ИКТ, а также осуществлять другие совместные меры по противодействию таким угрозам. Государствам, возможно, потребуется рассмотреть вопрос о разработке новых мер в этой сфере;

e. в процессе обеспечения безопасного использования ИКТ государства должны соблюдать положения резолюций 20/8 и 26/13 Совета по правам человека о поощрении, защите и осуществлении прав человека в Интернете и резолюций 68/167 и 69/166 Генеральной Ассамблеи о праве на неприкосновенность личной жизни в эпоху цифровых технологий, чтобы обеспечить всестороннее уважение прав человека, включая право свободно выражать свое мнение;

f. государство не должно осуществлять или заведомо поддерживать деятельность в сфере ИКТ, если такая деятельность противоречит его обязательствам по международному праву, наносит преднамеренный ущерб критически важной инфраструктуре или иным образом препятствует использованию и функционированию критически важной инфраструктуры для обслуживания населения;

g. государства должны принимать надлежащие меры для защиты своей критически важной инфраструктуры от угроз в сфере ИКТ, принимая во внимание резолюцию 58/199 Генеральной Ассамблеи о создании глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур и другие соответствующие резолюции;

h. государства должны удовлетворять соответствующие просьбы об оказании помощи, поступающие от других государств, критически важная инфраструктура которых становится объектом злонамеренных действий в сфере ИКТ. Государства должны также удовлетворять соответствующие просьбы о смягчении последствий злонамеренных действий в сфере ИКТ, направленных против критически важной инфраструктуры других государств, если такие действия проистекают с их территории, принимая во внимание должным образом концепцию суверенитета;

i. государства должны принимать разумные меры для обеспечения целостности каналов поставки, чтобы конечные пользователи могли быть уверены в безопасности продуктов ИКТ. Государства должны стремиться предупреждать распространение злонамеренных программных и технических средств в сфере ИКТ и использование пагубных скрытых функций;

j. государства должны способствовать ответственному представлению информации о факторах уязвимости в сфере ИКТ и делиться соответствующей информацией о существующих методах борьбы с такими факторами уязвимости, чтобы ограничить, а по возможности и устранить возможные угрозы для ИКТ и зависящей от ИКТ инфраструктуры;

k. государства не должны осуществлять или заведомо поддерживать деятельность, призванную нанести ущерб информационным системам уполномоченных групп экстренной готовности к компьютерным инцидентам (также именуемым группами готовности к компьютерным инцидентам или группам готовности к инцидентам в сфере кибербезопасности) другого государства. Государство не должно использовать уполномоченные группы экстренной готовности к компьютерным инцидентам для осуществления злонамеренной международной деятельности.

54 Генеральная Ассамблея ООН, *Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности*, A/70/174 (22 июля 2015), https://undocs.org/ru/A/70/174.

ПРИЛОЖЕНИЕ Б: НОРМЫ GCSC

1. НЕВМЕШАТЕЛЬСТВО В ПУБЛИЧНОЕ ЯДРО ИНТЕРНЕТА

НОРМА:

Государственные и негосударственные субъекты не должны вести или сознательно разрешать деятельность, которая преднамеренно и существенно наносит ущерб общедоступности или целостности публичного ядра Интернета и, следовательно, стабильности киберпространства.

ПРЕДПОСЫЛКИ

Дать определение публичному ядру Интернета — не самая простая задача, поскольку существует целый ряд разных типов атак, которые могут нанести ущерб общедоступности или целостности Интернета в широком смысле (результат, которого необходимо избегать). С учетом вышесказанного, можно все же выделить определенные компоненты, повреждение которых окажет максимальное негативное воздействие, и составить неисчерпывающий список подобных критически важных элементов. На высочайшем уровне Комиссия вкладывает в понятие «общедоступность» следующее значение — поведение субъекта оказывает существенное влияние на все слои населения. Таким образом, данная норма признает, что государства, которые ее поддерживают, могут участвовать в более ограниченной с точки зрения цели и масштаба деятельности, не оказывая при этом существенного влияния на все слои населения.

По определению Комиссии фраза «публичное ядро Интернета» подразумевает такие критически важные элементы инфраструктуры Интернета, как маршрутизация и передача пакетов, системы наименования и нумерации, криптографические механизмы обеспечения безопасности и идентификации, передающие среды, программное обеспечение и центры обработки данных.

К элементам маршрутизации и передачи пакетов относятся, в числе прочего, (1) оборудование, объекты, информация, протоколы и системы, способствующие передаче пакетированной коммуникации от источника до места назначения; (2) точки обмена интернет-трафиком (физические места, где обеспечивается доступ к Интернету); (3) пиринговые и ключевые маршрутизаторы основных сетей, предоставляющие пользователям возможность подключения; (4) системы, необходимые для обеспечения аутентичности маршрутизации и защиты сети от злоупотреблений; (5) цепочка проектирования, производства и поставки оборудования, используемого в вышеперечисленных целях; и (6) целостность самих протоколов маршрутизации и стандартизация их развития, а также процессы обслуживания.

К системам наименования и нумерации относятся, в числе прочего, (1) системы и информация, используемые в работе системы имен доменов в Интернете (включая реестры, имена серверов, контент зоны, инфраструктуру и процессы для криптографической подписи записей, такие как DNSSEC); (2) информационные сервисы WHOIS для корневой зоны, обратная иерархия адресов, код страны, географические и интернационализированные домены высшего уровня и новые общие и невоенные общие домены высшего уровня; (3) часто используемые публичные рекурсивные DNS-преобразователи; (4) системы органа присвоения номеров в Интернете и региональные интернет-регистраторы, которые обеспечивают доступ к уникальному размещению IP-адресов, номерам в автономной системе и IP-идентификаторам и обслуживают их; и (5) непосредственно протоколы наименования нумерации, целостность процессов стандартизации и результаты развития и обслуживания протоколов.

К криптографических механизмам обеспечения безопасности и идентификации относятся, в числе прочего, (1) криптографические ключи, используемые для аутенфикации пользователей и устройств и защиты интернет-транзакций; (2) оборудование, объекты, информация, протоколы и системы для производства, передачи, использования и депрекации этих ключей; (3) серверы управления ключами PGP, органы сертификации и инфраструктура сертификации открытых ключей; (4) система DANE и поддерживающие ее протоколы и инфраструктура; (5) механизмы отзыва сертификации и журналы прозрачности; (6) менеджеры паролей; (7) аутентификаторы доступа в роуминге; (8) механизмы определения точного времени и установления временного предшествования, такие как сетевой протокол синхронизации и его инфраструктура; (9) целостность процессов стандартизации и результаты развития и обслуживания криптографических алгоритмов и протоколов; и (10) цепочка проектирования, производства и поставки оборудования, используемого для внедрения криптографических процессов.

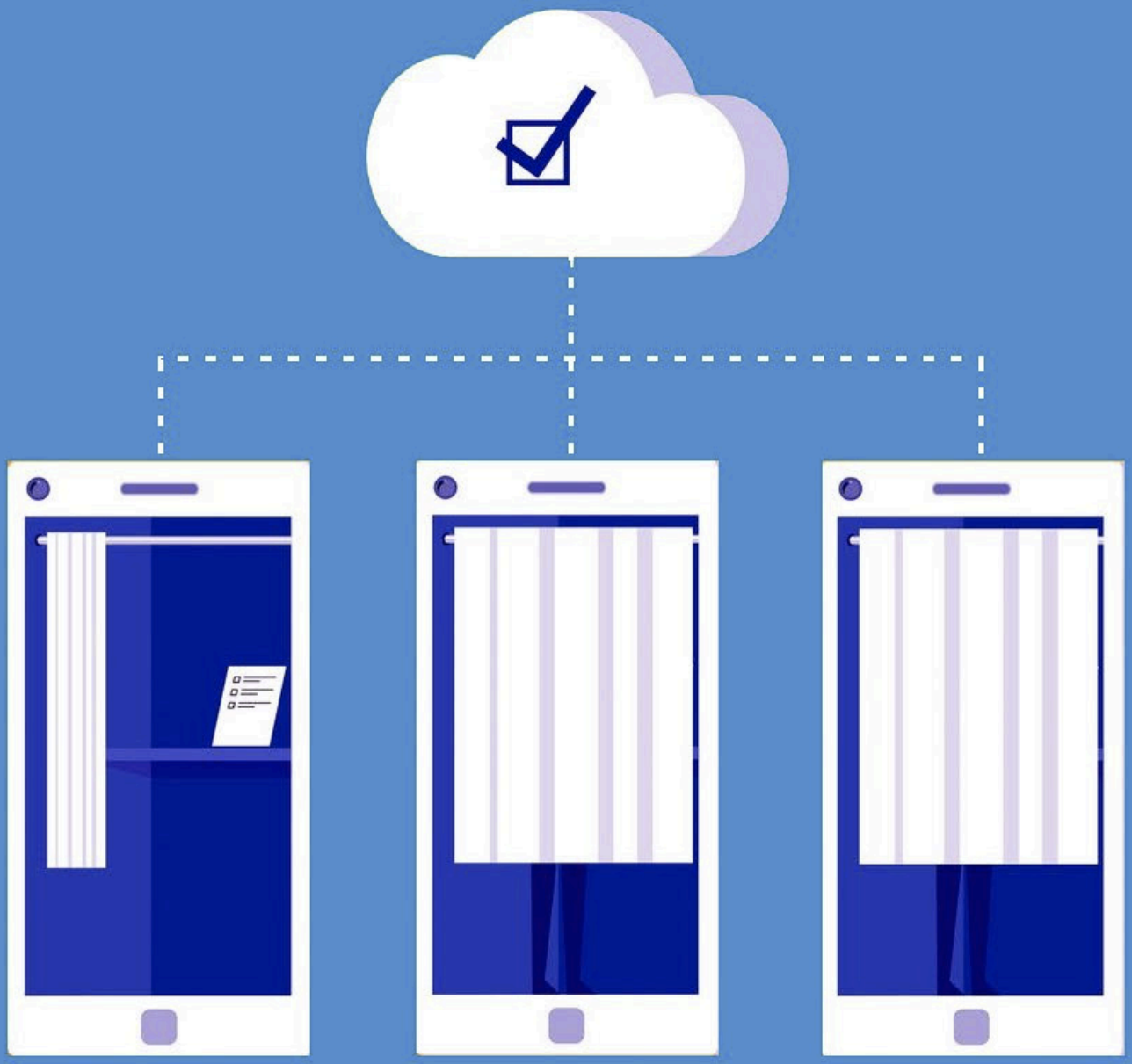
К передающим средам относятся, в числе прочего, (1) инфраструктура, системы и установки для общественных каналов коммуникации, будь то оптоволокно, медь или беспроводные каналы; (2) наземные и подводные кабели и наземные кабельные установки, центры обработки данных и другие поддерживающие их физические объекты; (3) сотовая и другая беспроводная голосовая коммуникация и обмен данными; (4) регулируемая и нерегулируемая широковещательная связь; (5) системы поддержки передачи, регенерации сигналов, выполнения перехода, уплотнения и выделения сигнала из шумов; и (6) кабельные системы, обслуживающие регионы или население в целом (кроме тех, которые обслуживают клиентов индивидуальных компаний).

К программному обеспечению относятся, в числе прочего, доступность и целостность процессов разработки, исходный код и инфраструктура распределения Patch-файлов программного обеспечения, используемого ядром Интернета и большими группами пользователей Интернета.

К центрам обработки данных относятся, в числе прочего, (1) физические объекты с серверами, контентом и интернет-инфраструктурой; (2) система для обеспечения безопасности центра обработки данных и управления физическим доступом к нему, операционные системы, системы управления, обслуживания и резервирования; и (3) коммуникационные системы, используемые для передачи связи из центра обработки данных и в него, а также в его пределах.

По мнению экспертов, защите подлежит гораздо большее число категорий Интернета и инфраструктуры на основе ИКТ, поэтому в будущем это определение может быть расширено.

2. ЗАЩИТА ИНФРАСТРУКТУРЫ ИЗБИРАТЕЛЬНЫХ СИСТЕМ



НОРМА:

Государственные и негосударственные субъекты не должны проводить, поддерживать или допускать кибероперации, направленные на нарушение нормальной работы технической инфраструктуры, необходимой для проведения выборов, референдумов или плебисцитов.

ПРЕДПОСЫЛКИ

Из всех правил, предписаний и принципов, регулирующих поведение стран в отношении взаимного признания прав и обычаев разными нациями, самой священной является, пожалуй, норма невмешательства. Статья 2(4) Устава ООН четко формулирует эту норму и закрепляет ее как законный и, следовательно, обязывающий принцип:

> Все Члены Организации Объединенных Наций воздерживаются в их 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 Объединенных Наций.

Этим положением составители Устава признают, что самая серьезная угроза принципу невмешательства исходит от принудительных мер, направленных против физической или политической автономии государства, поскольку оба эти фактора действительно критически важны для государственного суверенитета. Контролируемая государством территория может быть проявлением его суверенитета, но она не будет иметь значения без политической власти и независимости. Более того, ничто не отражает подлинную политическую независимость лучше, чем процессы, в которых участвует вся нация, — например, свободные и справедливые выборы. Устав ООН стремится обеспечить мощную защиту от ненадлежащего внешнего вмешательства. В цифровую эпоху эти защитные меры снова оказались в зоне риска.

Эксперты обсуждают, приравнивается ли кибервмешательство в выборы к незаконному нарушению суверенитета (поскольку такое поведение мешает исполнению неотъемлемой государственной функции) или к незаконному вмешательству. [55] Независимо от того, было ли нарушено международное право, существует явная возможность того, что нарушители — действуя в одиночку, группой или от имени целого государства — будут манипулировать выборами с помощью цифровых средств. Поскольку национальные коллективные процессы становятся все более сложными с точки зрения масштаба и изощренности, растет и объем данных, учреждений и инфраструктур для управления ими. Сегодня многие страны публикуют свои списки избирателей, обеспечивающие базовую, традиционную гарантию от манипуляций или мошенничества в ходе голосования, онлайн, подвергая подобные базы данных риску кибератак и незаконного использования. Аналогично, инструменты голосования используются в труднодоступных и удаленных уголках страны, операторы в которых могут быть не осведомлены обо всех рисках и проблемах, связанных с цифровыми манипуляциями. Поставщики программного обеспечения для голосования и компьютерные системы на местном «уровне кабины для голосования» также не защищены от вмешательств.

Принимая во внимание растущее число и интенсивность угроз для коллективных процессов и признавая неприемлемость подобных атак, GCSC рекомендует усилить национальные меры и повысить эффективность международного сотрудничества для предотвращения и смягчения кибервмешательств в техническую избирательную инфраструктуру, а также для реагирования на них. Комиссия признает, что обеспечение реального соблюдения соответствующих государственных законов на выборах или в других коллективных процессах на региональном, локальном или федеральном уровне остается четкой прерогативой конкретного государства. Тем не менее, кибератаки на избирательную инфраструктуру могут исходить от других стран, в связи с чем возникает необходимость найти решение для многостороннего сотрудничества. Все больше стран переводят свои избирательные механизмы в цифровой формат, поэтому множатся риски и уязвимости, связанные с такой инфраструктурой, как и множатся и угрозы масштабной кибератаки. Таким образом, государства должны воздерживаться от участия в кибероперациях против технической избирательной инфраструктуры другой страны. Рекомендуя данную норму, Комиссия подтверждает неприемлемость вмешательства в выборы независимо от того, считается оно нарушением международного права или нет.

55 Michael N. Schmitt, 'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law," *Chicago Journal of International Law*, Vol. 19, No. 1, and Nicholas Tsagourias, "Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace," https://www.ejiltalk.org/electoral-cyber-interfer ence-self-determination-and-the-princi-ple-of-non-intervention-in-cyberspace/.

3. НОРМА ДЛЯ ЗАЩИТЫ ОТ ВМЕШАТЕЛЬСТВА

НОРМА:

Государственные и негосударственные субъекты не должны вмешиваться или допускать вмешательство в разработку и производство товаров и услуг, если такое вмешательство может существенно нарушить стабильность киберпространства.

ПРЕДПОСЫЛКИ

В рамках нормы, охватывающей «невмешательство в публичное ядро Интернета», GCSC призывает государственные и негосударственные субъекты не причинять осознанный и существенный вред общедоступности или целостности публичного ядра Интернета. В поддержку этой нормы Комиссия отмечает растущую зависимость других инфраструктур от стабильного и безопасного Интернета и потенциально серьезные последствия сбоев в этой связи. В то время как норма о публичном ядре нацелена на «ядро Интернета», физические лица и организации сильно полагаются на определенные коммерческие продукты для доступа к этому публичному ядру и использования предлагаемых им возможностей соединения. В результате, вмешательство в ключевые компоненты программного и аппаратного обеспечения ИТ продуктов (включая, в числе прочего, операционные системы, промышленные системы управления, переключатели, маршрутизаторы и другое критически важное сетевое оборудование, ключевые криптографические продукты и стандарты, структуру микрочипа и широко применяемые приложения для конечных пользователей) может аналогичным образом лишить общество возможности безопасно пользоваться Интернетом и ослабить доверие к его исправному функционированию в целом. Такие атаки часто освещаются в новостях, но гораздо меньше внимания получает тот факт, что атака может состояться еще до выхода продукта или его обновления на рынок. Например, продукт может быть атакован путем включения в него уязвимости или скрытного изъятия функции защиты на этапе проектирования и производства или в ходе выполнения его обновления. Иными словами, вмешательство в продукт может произойти еще до его выхода на рынок или запуска в производство и иметь последствия для широкой общественности. Период между включением уязвимости и ее активацией для злонамеренного использования может быть разным.

Интересы и обязанности государства в отношении информационных технологий могут противоречить друг другу. С одной стороны, государство обязано развивать устойчивость и целостность киберинфраструктуры, помогать в предотвращении будущих кибератак со стороны нарушителей и способствовать укреплению безопасности цифровой экосистемы в целом. С другой стороны, государства имеют обязательство перед своими гражданами защищать национальную безопасность и бороться с преступниками и другими нарушителями кибербезопасности. Бывало так, что государства использовали уязвимости в цифровых продуктах и услугах, внедренные нарушителями, для поддержания национальной и общественной безопасности. Таким образом, поскольку государства считают использование уязвимостей эффективной мерой для исполнения своих обязанностей, они могут также посчитать полезным намеренное внедрение уязвимостей или лазеек в продукты и услуги, используемые нарушителями. Негосударственные субъекты тоже могут, в свою очередь, вмешиваться в продукты и услуги, нанося ущерб стабильности киберпространства в своих личных целях. Важно отметить, что эта норма запрещает вмешательство в продукты или услуги, которое может угрожать стабильности киберпространства. Данная норма не запрещает целенаправленные действия государства, не представляющие серьезного риска для общей стабильности киберпространства; например, целенаправленное ограниченное вмешательство в устройства конечного пользователя в целях военного шпионажа или уголовного расследования. Подобные действия, если они не происходят в рамках базовой инфраструктуры самого публичного ядра и не подрывают существенным образом доверие пользователей к Интернету в глобальных масштабах, едва ли ослабят общее доверие к киберпространству, которое является обязательным аспектом киберстабильности. Хотя ограниченное воздействие негосударственного субъекта на конкретные системы тоже допускается, следует отметить, что подобная деятельность может идти в разрез с применимыми положениями уголовного и гражданского права.

Государственные и негосударственные субъекты не должны в утвердительной форме вмешиваться в развитие или производство продуктов, но за предотвращение подобных действий отвечают также и сами представители отрасли. Таким образом, производители продуктов и услуг должны проявлять разумную осмотрительность при проектировании, разработке и поставке продуктов и услуг, отдавая приоритет безопасности и снижая вероятность возникновения, частоту, возможность использования и серьезность уязвимостей. Заинтересованные лица также должны отклонять любые явные попытки государственного или негосударственного субъекта скомпрометировать продукты или услуги, а также внедрить методы для сокращения риска вмешательств и реагирования в случаях обнаружения вмешательства.

4. НОРМА ДЛЯ ЗАЩИТЫ ОТ ИСПОЛЬЗОВАНИЯ УСТРОЙСТВ ИКТ В КАЧЕСТВЕ БОТНЕТОВ

НОРМА:

Государственные и негосударственные субъекты не должны распоряжаться ресурсами ИКТ широкой общественности для использования в качестве ботнетов или для аналогичных целей.

ПРЕДПОСЫЛКИ

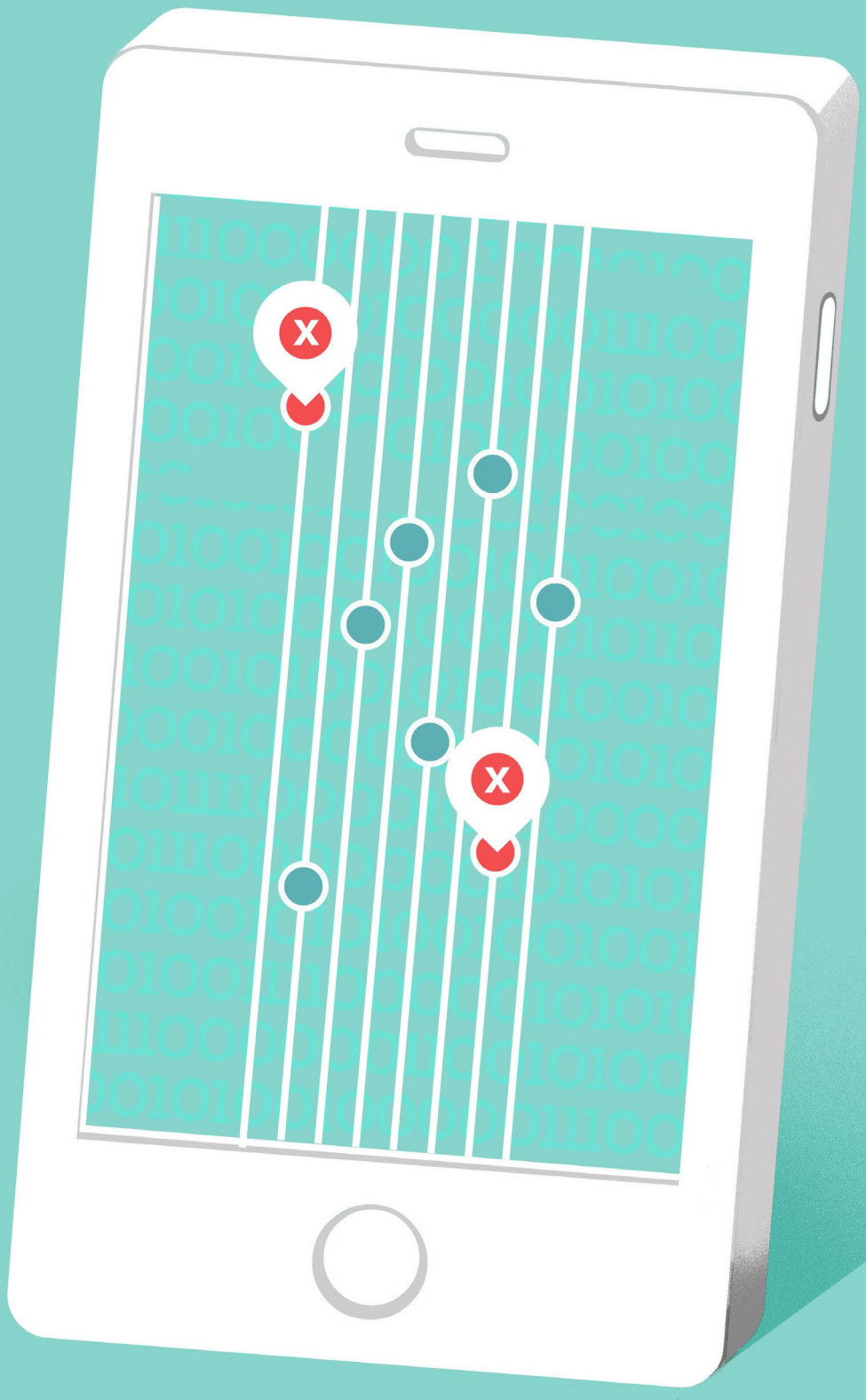
Устройства с выходом в Интернет становятся неотъемлемой частью жизни людей по всему миру. Мы окружены устройствами, имеющими невероятную массу возможностей — вычислительных, сетевых, измерительных и исполнительных. Термостаты, телевизоры, медицинские приборы, будильники и автомобили имеют вычислительный, аккумулирующий и сетевой потенциал, который можно присвоить и злонамеренно эксплуатировать. Использование уязвимостей в базовом коде таких устройств может привести к угрозам физической безопасности лиц, использующих эти устройства: прибор, работающий за пределами заданных параметров, может загореться или создать другую опасную ситуацию — например, внезапное открытие дверцы автомобиля, видеотрансляция из дома или неисправность медицинского оборудования.

Установку программных агентов, массово или без разрешения, для использования вычислительных, аккумуляционных или сетевых ресурсов устройства мы называем ботнетами. Эти ботнеты могут использоваться для прямого воздействия на разные конкретно выбранные системы и влиять, например, на конфиденциальность, доступность и целостность данных конечной цели. Таким образом, теоретически незадействованное стороннее устройство и его владелец/оператор без своего ведома становятся участниками незаконной кибератаки. Разрешение установить на устройстве вредоносные программные агенты не только делает устройство более уязвимым перед другими атаками (например, со стороны преступников) или вмешательствами в нормальное функционирование устройства, но и делает владельца/оператора этого устройства потенциально ответственным за ущерб, нанесенный конечной цели. Это особенно актуально в ситуациях, когда компрометирование устройства может непреднамеренно сделать устройство и его владельца/оператора невольными соучастниками межгосударственной вражды и повлечь за собой санкции или ответственность.

Мы все больше полагаемся на технологии в нашей повседневной жизни, все больше устройств с доступом к Интернету появляется на рынке, и в этих условиях использование бытовых устройств в качестве ботнетов сильно подрывает доверие и дестабилизирует общество. Комиссия признает, что бывают ситуации — например, когда речь идет об обеспечении правопорядка — в которых уполномоченным государственным субъектам может потребоваться установить программные агенты на устройства конкретного нарушителя или группы нарушителей. Тем не менее, государственные и негосударственные субъекты не должны распоряжаться гражданскими устройствами широкой общественности (массово) для поддержки и непосредственного осуществления кибератак независимо от исходной мотивации. [56]

56 Эта норма дополняет ранее предложенную норму о том, что государственные и негосударственные субъекты не должны вмешиваться в продукты перед их выпуском. Предыдущая норма нацелена в большей степени на цепочку поставок, тогда как данная норма охватывает уже выпущенные устройства.

5. НОРМА, ПРЕДПИСЫВАЮЩАЯ ГОСУДАРСТВАМ РАЗРАБОТАТЬ ПРОЦЕСС ОЦЕНКИ УЯЗВИМОСТЕЙ



НОРМА:

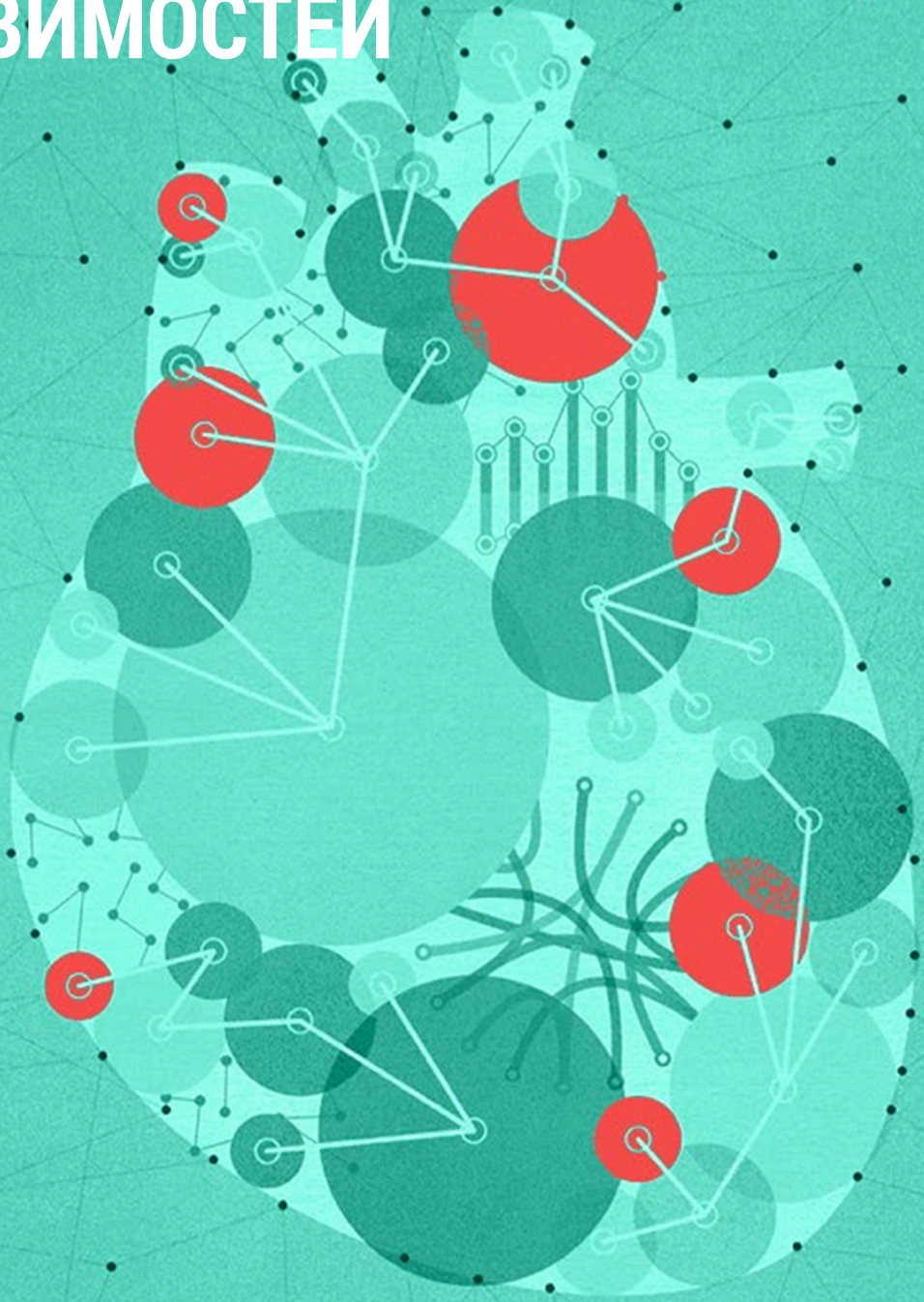
Государства должны создать прозрачные с процедурной точки зрения методики, позволяющие оценивать, когда следует (и следует ли) сообщать общественности об уязвимостях или недостатках информационных систем или технологий. По умолчанию подобные сведения всегда следует обнародовать.

ПРЕДПОСЫЛКИ

По мере усложнения операционных систем, критически важного программного обеспечения и компьютерных аппаратных средств число уязвимостей в них растет. Эти уязвимости могут быть использованы государственными и негосударственными субъектами. Интересы и обязанности государства, обнаружившего новые уязвимости, могут противоречить друг другу. С одной стороны, государство обязано развивать устойчивость и целостность инфраструктуры, необходимой для обеспечения стабильности киберпространства, и помогать в предотвращении злонамеренной киберактивности, чтобы сделать всю цифровую экосистему более безопасной для всех пользователей. Эта обязанность подразумевает, что государство должно оперативно сообщить о новой уязвимости поставщикам и производителям, чтобы они устранили ее, а также сделать более массовые публичные заявления, когда это уместно, для защиты общественности. С другой стороны, государство обязано защищать своих граждан от преступников, расследовать киберпреступления и привлекать к ответственности за них. Кроме того, государство вправе налагать санкции, выступающие одновременно в качестве специального и общего сдерживающего фактора для будущих злонамеренных деяний. Крайне важный инструмент для преследования нарушителей, особенно таких искушенных, как государства-изгои, — это использование уязвимостей в цифровой инфраструктуре, на которую они полагаются. Таким образом, государства часто пытаются доказать, что они должны сохранить хотя бы некоторые возможности, включая использование неуказанных уязвимостей, иначе крайне опытные нарушители смогут остаться не раскрытыми и не проверенными.

Хотя государства вряд ли будут добровольно сообщать об всех обнаруженных уязвимостях, недавно возникло движение нескольких стран за то, чтобы разглашать выявленные уязвимости в интересах более масштабной систематической кибербезопасности, а не замалчивать их. Ключевой фактор успеха здесь — это формирование государствами общедоступного процесса оценки преимуществ и недостатков подобного разглашения с учетом полного спектра политических, экономических, социальных и технических аспектов. Если говорить более конкретно, этот процесс должен иметь прозрачную процедуру и учитывать весь спектр таких факторов, как: безопасность и устойчивость сети, безопасность пользователей и их данных, правоохранительная деятельность и национальная безопасность, а также дипломатические и коммерческие аспекты. США недавно опубликовали новую версию данного процесса, и другие страны подумывают о формировании собственных политик в рамках процесса оценки уязвимостей (VEP). Учитывая, что обнаружение и разглашение уязвимостей выходит далеко за рамки какого-либо государства, для развития устойчивости сети и одновременного обеспечения национальной безопасности каждой стране не помешает разработать собственный подобный процесс в интересах долгосрочной стабильности киберпространства. Кроме того, государства должны стремиться к обеспечению совместимости и предсказуемости своих процессов. Существование данных процессов может сработать в качестве меры выстраивания доверия между государствами в том смысле, что такие процессы дают определенную гарантию того, что соответствующие аспекты и противоречащие интересы полностью учтены. Разумеется, разные страны имеют разные возможности и уникальные межведомственные структуры. Тем не менее, любой эффективный процесс VEP должен учитывать широкий спектр точек зрения и аспектов. Кроме того, несмотря на то, что реальные решения по конкретным ситуациям могут при необходимости оставаться конфиденциальными, необходимо обеспечить прозрачность общих процедур и алгоритма принятия таких решений. Наконец, эта норма охватывает не только формирование процесса принятия решений о разглашении. Если государство или любой другой субъект решит разгласить уязвимость, это необходимо сделать в ответственной манере, для повышения общественной безопасности и без предоставления возможности воспользоваться этой уязвимостью.

6. НОРМА ДЛЯ СНИЖЕНИЯ И СМЯГЧЕНИЯ СУЩЕСТВЕННЫХ УЯЗВИМОСТЕЙ



НОРМА:

Разработчики и производители продуктов и услуг, от которых зависит стабильность киберпространства, должны (1) отдавать приоритет безопасности и стабильности; (2) предпринимать разумные шаги для обеспечения того, чтобы их продукты или услуги не подвергались значительной уязвимости; и (3) своевременно принимать меры в отношении уязвимостей, которые обнаруживаются впоследствии, и обеспечивать прозрачность этих мер. Все участники обязаны обмениваться информацией об уязвимостях, чтобы помочь предотвратить или смягчить злонамеренную киберактивность.

ПРЕДПОСЫЛКИ

Определенные ИТ-продукты и услуги жизненно важны для обеспечения стабильности киберпространства в связи с тем, что они используются в ключевой технической инфраструктуре, например, в разрешении ключевых имен и маршрутизации, поскольку их распространенность улучшает опыт интернет-взаимодействия или из-за их применения в критически важных инфраструктурах. Производители продуктов и услуг должны проявлять разумную осмотрительность при проектировании, разработке и поставке продуктов и услуг, отдавая приоритет безопасности и снижая вероятность возникновения, частоту, возможность использования и серьезность уязвимостей.

В связи с растущей сложностью программного и аппаратного обеспечения уязвимости в соответствующих продуктах уже стали фактом жизни. Как правило, эти уязвимости являются непреднамеренными, но злонамеренные государственные и негосударственные субъекты зачастую используют их для подрыва стабильности киберпространства.

Более того, в объединенном киберпространством и зависящем от него мире обнаруженная уязвимость может повлиять на целый ряд продуктов и услуг разных производителей и в разных средах. Восстановление одного продукта без разглашения другим лицам его основной уязвимости может защитить этот продукт, но не стабильность киберпространства в целом. Те, кто лучше всего может оценить последствия конкретной уязвимости, — это, как правило, те, кто разрабатывает, производит, устанавливает и эксплуатирует продукты, на которые влияют эти уязвимости. Важно делиться информацией, которая помогает устранить уязвимости в сфере безопасности или предотвратить, ограничить или смягчить атаку. [57]

Пока что очень непросто обеспечить полное отсутствие уязвимостей в недавно выпущенных или обновленных продуктах, поэтому предложенная норма, скорее призывает тех, кто участвует в разработке или производстве таких продуктов, предпринимать «разумные меры» для снижения частоты и серьезности тех уязвимостей, которых все-таки не удается избежать.

В то время как норма «невмешательства» касается намеренного включения уязвимостей в критически важные продукты и услуги, а норма обеспечения кибергигиены, по большому счету, затрагивает обязанности конечных пользователей, предложенная норма призывает тех, кто участвует в разработке или производстве критически важных продуктов, предпринимать «разумные меры» для снижения частоты и масштабности серьезных уязвимостей и для своевременного и эффективного смягчения их последствий, а также для их разглашения в тех случаях, когда это уместно. Применимый процесс должен быть прозрачным, предсказуемым и стабильным.

57 В одной из норм ответственного поведения государств в докладе Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности в 2015 году (A/70/174) утверждается, что «государства должны способствовать ответственному представлению информации о факторах уязвимости в сфере ИКТ и делиться соответствующей информацией о существующих методах борьбы с такими факторами уязвимости, чтобы ограничить, а по возможности и устранить возможные угрозы для ИКТ и зависящей от ИКТ инфраструктуры».

7. НОРМА О БАЗОВОЙ КИБЕРГИГИЕНЕ КАК ФУНДАМЕНТАЛЬНОМ ЭЛЕМЕНТЕ ЗАЩИТЫ

НОРМА:

Государства должны принимать соответствующие меры, в том числе утверждать законы и правовые нормы, которые будут гарантировать элементарную гигиену киберпространства.

ПРЕДПОСЫЛКИ

По мере распространения Интернета по миру и его проникновения во все аспекты современной жизни пользователи всех видов — физические лица, организации, предприятия и органы власти — все больше полагаются на технологии и доступ к информации из Интернета. Политические, экономические, информационные, образовательные, развивающие и все остальные формы социального взаимодействия практически полностью зависят от Интернета и сопутствующих технологий. Тем не менее, это «современное чудо» остается, по большому счету, небезопасным, и жертвой его угроз может стать каждый.

Консенсус в отношении наиболее эффективных способов оптимизации многообещающих технологий киберпространства при одновременной защите общественности все еще не достигнут. И все же, большинство признает, что преимущества наших объединенных в цифровой среде жизней не могут устойчиво развиваться без согласованных стандартов для обеспечения базовой безопасности в киберпространстве. В связи с этим комиссия горячо поддерживает широкомасштабное принятие и подтвержденное внедрение базовых принципов кибергигиены — то есть, свода фундаментальных мер, представляющих собой приоритетные, жизненно важные задачи для защиты от, предотвращения и оперативного смягчения тех угроз в киберпространстве, которых можно избежать.

Действительно, с учетом обширности взаимосвязанного онлайн-пространства соблюдение этих мер должно являться базовой обязанностью всех пользователей. Кибергигиена должна охватывать утвержденные надежные меры по внедрению норм, широкому обмену технической информацией и лучшими практиками, а ее соблюдение должно надлежащим образом контролироваться. Для всех более продвинутых устройств и процессов требуются не менее продвинутые законы и нормы. Увеличивая масштаб ответственности за соблюдение этих основных принципов киберзащиты, государства не должны препятствовать инновациям или менять базовые свойства Интернета.

Стандарты кибергигиены уже существуют в разной форме. [58] Они становятся все более распространенными на международном уровне, поскольку все больше государств и организаций начинают осознавать важность принятия мер по предотвращению и оперативному смягчению угроз со стороны известных вредоносных программных средств. Более того, эти стандарты представляют собой передовую практику, подчеркивают важность разумного и регулярного контроля и оспаривают значимость автоматизированного обмена информацией при наличии возможности оповестить пользователей о проблеме. Данные базовые меры киберзащиты свидетельствуют о том, что ни одно государство, организация или группа пользователей не смогут в одиночку устранить все риски, связанные с киберпространством. Кроме того, согласно формулировкам этих мер, в укреплении кибербезопасности играют роль пользователи всех уровней.

По мнению GCSC, фундаментальная защита кибербезопасности через широкое принятие мер кибергигиены исключительно важна для обеспечения ответственного использования и благоприятного развития Интернета. Обеспечение безопасности должно восприниматься как непрерывный процесс, где обязанности распределены между всеми участниками и где имеются соответствующие механизмы, такие как автоматическая отчетность и обмен информацией, для надлежащего привлечения к ответственности.

Комиссия также признает, что многие страны мира сталкиваются с серьезными проблемами при использовании информационных и коммуникационных технологий, и призывает государства делиться знаниями и предлагать помощь для реализации процессов эффективного внедрения базовых принципов кибергигиены в целях расширения охвата этой нормы.

58 Это включает, в числе прочих, Европейский институт телекоммуникационных стандартов (ETSI), некоммерческий Центр Интернет-безопасности (CIS) и Управление радиотехнической обороны Австралии (ASD).

8. НОРМА ПРОТИВ АТАКУЮЩИХ КИБЕРОПЕРАЦИЙ СО СТОРОНЫ НЕГОСУДАРСТВЕННЫХ СУБЪЕКТОВ

НОРМА:

Негосударственные субъекты не должны участвовать в атакующих кибероперациях, а государственные структуры должны предотвращать подобные действия и реагировать в тех случаях, если они совершаются.

ПРЕДПОСЫЛКИ

Информационные и коммуникационные технологии изменили наши жизни в лучшую сторону, но вместе с тем привнесли в них новые угрозы безопасности. Скорость и повсеместность кибероперацій зачастую порождают существенные сложности для государственных судебных систем и сотрудничества в сфере охраны международного права. Несмотря на эти трудности необходимо помнить, что государственный суверенитет является краеугольным камнем основанной на правилах международной системы мира и безопасности. Государства имеют монополию на законное применение силы в строгом соответствии с нормами международного права. Некоторые негосударственные субъекты, в основном, частные компании, выступают за право проводить атакующие кибероперации за пределами государственных границ, заявляя о том, что такое поведение может быть необходимо для оборонной деятельности, поскольку у государств нет достаточного потенциала для защиты от киберугроз. Подобные атакующие кибероперации негосударственных субъектов иногда завуалированно называют «активной киберзащитой», [59] включая в это понятие, в числе прочего, так называемые «ответные хакерские атаки», проводимые в оборонных целях.

Некоторые государства не контролируют или активно игнорируют эти практики, несмотря на риски, которые они могут навлечь на стабильность и безопасность киберпространства. Тем не менее, во многих странах подобные практики считаются пусть и не преступными, но незаконными, в других же они как будто не запрещены, но и не разрешены в явной форме. Вместе с тем, есть страны, которые расценивают возможность легализации атакующих кибероперацій негосударственных субъектов. Действительно, некоторые государства приняли решение или внесли предложение о легализации атакующих кибероперацій негосударственных субъектов на государственном уровне.

По мнению GCSC, такая практика подрывает стабильность киберпространства. Она может привести к серьезным сбоям и ущербу, в том числе, для третьих сторон, а также спровоцировать сложную юридическую полемику и вызвать обострение конфликтов. Государства, которые в явной форме соглашаются с подобной практикой или осознанно разрешают негосударственным субъектам проводить атакующие кибероперации в своих личных целях или в целях третьих сторон, создают опасный прецедент и рискуют нарушить нормы международного права. Комиссия убеждена, что атакующие меры необходимо ограничивать пределами государства, и призывает международное сообщество установить строгие и всеобъемлющие принципы, регулирующие реагирование государств на враждебные действия и применимые также и к кибероперациям. Аналогичным образом, согласно нормам международного права негосударственные субъекты, действующие от имени государств, должны расцениваться как их агенты и, следовательно, считаться элементами государства. [60]

Допуская такую практику, государство может быть привлечено к ответственности согласно нормам международного права. [61] Государства должны предотвращать атакующие кибероперации негосударственных субъектов как на национальном, так и на международном уровне.

59 Активная киберзащита подразумевает совокупность мер от самообороны в сети жертвы до разрушительной деятельности в сети атакующего. Атакующие кибероперации в данном контексте означают, что обороняющийся действует за пределами своей сети, независимо от того, каковы его намерения (нападение или защита), и независимо от юридической классификации этих действий. Определения атакующих кибероперацій и активной киберзащиты будут доработаны.

60 Ознакомиться с «дополнительным положением» о более широком трактовании этой ситуации в рамках международного права можно здесь: https://cyberstability.org/wp-content/uploads/2018/11/Additional-Note-to-the-Norm-Against-Offensive-Cyber-Operations-by-Non-state-Actors-Norm-Package-Singapore.pdf.

61 Там же

ПРИЛОЖЕНИЕ B: ИСТОРИЯ, ЦЕЛИ И ПРОЦЕССЫ GCSC

С момента своего основания в феврале 2017 года на Мюнхенской конференции по безопасности под патронажем голландского министра иностранных дел Берта Кундерса Глобальная комиссия по стабильности киберпространства остается одной из главных многосторонних инициатив такого рода, созданной специально для обеспечения стабильности киберпространства. Комиссия, сопредседателями которой являются Майкл Чертофф, бывший министр внутренней безопасности США, Лата Редди, бывший заместитель советника по национальной безопасности Индии; а ранее и Марина Кальюранд, член Европарламента и бывший министр иностранных дел Эстонии, имеет в своем составе 28 выдающихся личностей из разных стран и с разным опытом в области международной кибербезопасности. [62] Деятельность Комиссии поддерживает группа специальных советников — Секретариат, состоящий из *Гаагского* центра стратегических исследований (HCSS), EastWest Institute (EWI), исследовательской консультативной группы, а также партнеров и спонсоров, включая Министерства иностранных дел Нидерландов и Франции, Агентство по кибербезопасности Сингапура, Microsoft, Общество Интернета и Afilias.

Комиссия возникла из желания не распускать предыдущие комиссии гражданского общества, включая Глобальную комиссию по управлению Интернетом, и объединить их усилия с деятельностью Глобальной конференции по киберпространству (GCCS). В 2015 году *Гаагскому* центру стратегических исследований (HCSS) было поручено организовать подготовительную сессию для Гаагского собрания комиссии GCCS, задача которой — обеспечение международного мира и безопасности. Многие существенные положения разработанной впоследствии декларации GCCS опирались непосредственно на результаты этой подготовительной встречи и однозначно указывали на необходимость многостороннего формата для обсуждения вопросов международной кибербезопасности. Кроме того, HCSS сформировал ключевую группу организаций, оказывающих содействие комиссии и спонсоров (изначально в нее входили Microsoft, Общество Интернета и Министерство иностранных дел Нидерландов) и разработал стратегический план. В августе 2016 года, заполучив поддержку EastWest Institute (EWI) как партнера в Секретариате, HCSS организовал собрание для GCSC Inception Group в гарвардской школе управления имени Джона Ф. Кеннеди, где был составлен проект основных требований к работе GCSC, вступлению в нее, ее структуре и целям, а также сформулирована миссия Глобальной комиссии по стабильности киберпространства.

Миссия звучит следующим образом:

> Целью создания Глобальной комиссии по стабильности киберпространства (GCSC) является разработка норм и принципов, призванных повышать безопасность и стабильность киберпространства на международном уровне, а также регулировать деятельность государственных и негосударственных субъектов в киберпространстве. GCSC задействует всех заинтересованных лиц для развития общего понимания применяемых концепций. Работа данной комиссии, которая поддерживает исследования, обмен информацией и наращивание потенциала, позволит усовершенствовать киберстабильность.

С самого начала GCSC была задумана как инструмент влияния на вопросы международного мира и безопасности, связанные с киберпространством и обычно обозначаемые как «международная кибербезопасность». Наш партнер Inception Group отметил необходимость сбора разных мнений, в частности, от сообществ по управлению Интернетом и технических сообществ, и учета этих мнений в текущих дискуссиях о международной кибербезопасности. Цель такого подхода — обеспечить более обширную информационную базу для дискуссий в сфере контроля вооружения и в сообществах по укреплению мира и безопасности, где недостаточная вовлеченность гражданского общества и частного сектора оказывает сильное влияние на результаты работы, особенно над нормами. В связи с этим многосторонний подход был отнесен в категорию практических, а не идеологических задач.

62 Полный список членов комиссии можно найти на стр. 4.

В своих обсуждениях GCSC руководствуется принципом «сверху-вниз и снизу-вверх». Во-первых, комиссия выделила практические нормы, отвечающие самым актуальным и острым нуждам в сфере международной кибербезопасности, которые были озвучены членами комиссии, и решение для которых еще не было предложено никакой другой организацией. Во-вторых, она сформулировала из новых и уже существующих норм рабочее определение киберстабильности и ее основных принципов. В-третьих, была разработана концепция стабильности для более четкого понимания того, что требуется архитектуре международного мира и безопасности для соответствия этому определению. Наконец, комиссия разработала рекомендации по достижению поставленных ею целей для государственных и негосударственных субъектов.

Обсуждение членами комиссии этих целей выходило за пределы географических границ и проводилось между разными группами заинтересованных сторон. Комиссия с самого начала делает акцент на проведение своих собраний в связке с актуальными конференциями, чтобы привлечь как можно больше разных заинтересованных сторон [63] Кроме того, комиссия активно привлекает к участию в своей работе исследовательские группы и широкую общественность. Для объединения усилий GCSC с деятельностью более обширного научного сообщества была создана исследовательская консультативная группа с председателем и четырьмя заместителями, [64] которая управляет электронной рассылкой для списка из более чем 200 экспертов. Кроме того, исследовательская консультативная группа заложила основу для широкомасштабной исследовательской программы, в рамках которой было инициировано свыше 20 проектов исследовательских институтов и отдельных лиц по всему миру. [65] Основной объем проделанной работы был представлен членам комиссии на специально организованном для этого «Заседании по киберстабильности».

Перед публикацией данного отчета и ранее выпущенных норм комиссия последовательно привлекала к участию в своей работе широкий круг заинтересованных сторон из числа государственных субъектов, представителей гражданского общества и промышленности. Распределяя задачи по всем категориям комиссии мы смогли обеспечить непрерывный приток мнений и комментариев со стороны. Онлайн-просьбы о консультациях были опубликованы в отношении норм GCSC и определения киберстабильности. Из разных уголков мира было получено свыше 23 откликов, которые помогли сформировать информационную базу для дискуссий комиссии. Более того, комиссия приняла активное участие более чем в 70 конференциях и мероприятиях, провела ряд круглых столов, сопутствующих мероприятий и специальное заседание по киберстабильности с привлечением множества государственных и негосударственных субъектов.

Наконец, сами члены комиссии установили и поддерживают активную связь с соответствующими местными сообществами. Отклики и обратная связь от этих групп легли в основу взаимодействия с более широким кругом государственных и негосударственных экспертов, а также помогают сформировать базу сторонников дальнейшей работы над этим отчетом.

63 Официальные собрания комиссии проходили на следующих мероприятиях: Мюнхенская конференция по безопасности 2017 (Мюнхен, Германия); CyCon (Таллин, Эстония); BlackHat USA (Лас-Вегас, США); Глобальная конференция по киберпространству (Нью-Дели, Индия); Международный форум по кибербезопасности (FIC) 2018 (Лилль, Франция); Мюнхенская конференция по безопасности 2018 (Мюнхен, Германия — присуждение наград); GLOBSEC (Братислава, Словакия); Cyber Week (Тель-Авив, Израиль — присуждение наград); International Cyber Week (Сингапур); Парижский мирный форум и Форум по управлению Интернетом (Париж, Франция — присуждение наград); Институт ООН по исследованию проблем разоружения 2019 (Женева, Швейцария); Общественный форум ICANN 64 (Кобе, Япония); EuroDIG (Гаага, Нидерланды); Ежегодный Глобальный форум по вопросам киберпространства (Аддис-Абеба, Эфиопия).

64 В тематический охват группы входят четыре категории: международный мир и безопасность, международное право, управление Интернетом и технология.

65 См. раздел «Благодарности».

БЛАГОДАРНОСТИ

Глобальная комиссия по стабильности киберпространства (GCSC) хотела бы поблагодарить множество учреждений и отдельных лиц, которые оказали поддержку работе комиссии и внесли свой вклад, включая, в числе прочих, наших спонсоров, исследовательскую консультативную группу, авторов исследовательских работ и рецензентов, а также ассистентов. Ниже перечислены некоторые из тех, кто способствовал успеху комиссии.

Секретариат

ГААГСКИЙ ЦЕНТР СТРАТЕГИЧЕСКИХ ИССЛЕДОВАНИЙ (HCSS)

Александр Климбург, руководитель Секретариата Глобальной комиссии по стабильности киберпространства
Лаук Фасен, руководитель проектов Секретариата Глобальной комиссии по стабильности киберпространства
Эллиот Мейхью, помощник руководителя проектов Секретариата Глобальной комиссии по стабильности киберпространства

При дополнительной поддержке:
Тимон Домела Ньивенхёйс Нигард, **Кун ван ден Дол**, **Нилс Ренсен** и **Кая Карлсон**.

EASTWEST INSTITUTE (EWI)

Брюс Макконнелл, соруководитель Секретариата Глобальной комиссии по стабильности киберпространства
Аннелен Рогеман, руководитель проектов секретариата Глобальной комиссии по стабильности киберпространства

При дополнительной поддержке: **Эбигейл Лоусон**, **Драган Стояновски** и **Конрад Ярзенбовски**.

Партнеры, спонсоры и организации, оказывающие содействие комиссии

Гаагский центр стратегических исследований (HCSS), EastWest Institute (EWI) и члены комиссии выражают благодарность следующим организациям за их поддержку:

ПАРТНЕРЫ:

- **Министерство иностранных дел Нидерландов**, **Тимо Костер** и **Димитри Вогелар**
- **Microsoft**, **Ян Нойтце** и **Кая Сиглик**
- **Агентство по кибербезопасности Сингапура**, **Дэвид Кох** и **Ситурадж Понрадж**
- **Общество Интернета (ISOC)**
- **Министерство иностранных дел Франции**, **Анри Вердье** и **Дэвид Мартинон**
- **Afilias**, **Рам Мохан** и **Филипп Грабензее**

СПОНСОРЫ:

- **Министерство иностранных дел Швейцарии**
- **GLOBSEC**
- **Министерство иностранных дел Эстонии**
- **Министерство внутренних дел и коммуникаций Японии**

ОРГАНИЗАЦИИ, ОКАЗЫВАЮЩИЕ СОДЕЙСТВИЕ КОМИССИИ:

- **Комиссия Африканского союза**
- **Конференция Black Hat USA**
- **Конференция DEF CON**
- **Представительство Европейского Союза в ООН в Женеве**
- **Глобальный форум по вопросам киберпространства**
- **Google**
- **Муниципалитет Гааги**
- **Packet Clearing House**
- **Тель-Авивский университет**
- **Институт ООН по исследованию проблем разоружения**

Эти организации и институты работают над развитием дискуссии и выдвижением креативных решений для наиболее острых проблем в отношении стабильности киберпространства.

Исследователи

Комиссия выражает благодарность членам исследовательской консультативной группы, которая насчитывает более 200 онлайн-участников и которая включила GCSC в более масштабное научное сообщество. В частности, мы хотим поблагодарить исследователей, которым было поручено написать брифинги и протоколы дискуссий членов комиссии.

БРИФИНГ GCSC 1 (НОЯБРЬ 2017)

Алекс Григсби, Бывший член Совета по международным отношениям (CFR)
Дебора Хоузен-Курье, Konfidas Digital Ltd.
Джоанна Кулеша, Лодзинский университет
и **Рольф Х. Вебер**, Цюрихский университет
Олувафеми Ошо, **Йосеф А. Оенийи**, и **Шафи Абдулхамид**, Федеральный технологический университет, Минна
Аналия Аспис, университет Буэнос-Айреса, **Роберт Моргус**, бывший член аналитического центра «Новая Америка»,
Макс Смитс, бывший член Стэнфордского центра международной безопасности и сотрудничества и **Трей Герр**, Школа управления им. Джона Ф. Кеннеди
Арун Мохан Сукумар, **Мадхулика Срикумар**,
и **Бедавьяса Моханти**, Observer Research Foundation (ORF)

БРИФИНГ GCSC 2 (МАЙ 2018)

Шень И, **Цзян Тяньцзяо**, и **Ван Лэй**, Исследовательский центр регулирования киберпространства университета Фудань
Элана Бройтман, **Майлин Фидлер**, и **Роберт Моргус**, бывшие члены аналитического центра «Новая Америка»
Иллонай Хикок и **Ариндражит Басу**, Центр Интернета и общества
Томас Юрен, **Барт Хогевен**, и **Фергус Хансон**, Австралийский институт стратегической политики (ASPI)
Драган Младенович и **Владимир Радунович**, DiploFoundation
Томас Райнхольд, Институт по исследованию проблем мира и политики в области безопасности Гамбургского университета

Консультации

Комиссия хотела бы поблагодарить следующие лица и организации за активную обратную связь в ответ на Просьбу о консультациях в отношении сингапурского пакета норм (с 17 декабря 2018 года по 17 января 2019 года) и в рамках инициативы по определению стабильности киберпространства (с 14 августа 2019 года по 6 сентября 2019 года):

Хусейн Абул-Энин, Access Partnership
Кайоде Аканни, DesignIT
Джонатан Д. Аронсон, университет Южной Калифорнии (USC)
Авирам Ацаба, Национальный Кибердиректорат Израиля
Ариндражит Басу, **Гуршабад Гровер**, **Иллонай Хикок**, и **Каран Сайни**, Центр Интернета и общества
Витаутас Бутримас, Центр изучения передового опыта НАТО в области энергетической безопасности
Технологическое соглашение по кибербезопасности
Майкл Дэниэл, Cyber Threat Alliance
Global Partners Digital
Арвинд Гупта и **Дики Кумар**, Vivekananda International Foundation
Тара Хэйрстон и **Анастасия Казакова**, Kaspersky
Свен Герпиг, Stiftung Neue Verantwortung
Дрю Митник, Access Now
Джордж М. Мур, Центр изучения вопросов нераспространения ядерного оружия им. Джеймса Мартина
Бретт ван Никерк и **Тришана Рамлукан**, университет Квазулу-Натал
Питер Свайр, **Джастин Хеммингс**, и **Сриниди Сринивасан**, Georgia Tech Scheller College of Business
Ян де Витт, Siemens/TU Delft

Наконец, комиссия хотела бы поблагодарить следующих экспертов, чья работа и знания направляли обсуждения в рамках комиссии и обеспечивали для них информационную базу:

Деннис Брудерс, Лейденский университет
Дебора Браун и **Вероника Феррари**, Ассоциация прогрессивных коммуникационных технологий (Association for Progressive Communications)
Майкл Дэниэл, Cyber Threat Alliance
Франсуа Делерю, Институт стратегических исследований военной школы Министерства обороны Франции (IRSEM)
Акхил Део и **Арун Мохан Сукумар**, Observer Research Foundation (ORF)
Марта Финнемор, университет Джорджа Вашингтона
Оде Жери, университет Руана
Дункан Холлис, юридический факультет университета Темпл
Джоанна Кулеш, Лодзинский университет
Питер Роулэнд, Packet Clearing House
Майкл Шмидт, юридический факультет университета Эксетера

Patra Kongsirimongkolchai / EyeEm / Getty Images

СЕКРЕТАРИАТ

The Hague Centre for Strategic Studies

EastWest INSTITUTE

ПАРТНЕРЫ

Ministry of Foreign Affairs of the Netherlands

CSA SINGAPORE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

Internet Society

Microsoft

Afilias

СПОНСОРЫ

Министерство иностранных дел Швейцарии

GLOBSEC

Министерство иностранных дел Эстонии

Министерство внутренних дел и коммуникаций Японии

ОРГАНИЗАЦИИ, ОКАЗЫВАЮЩИЕ СОДЕЙСТВИЕ КОМИССИИ

Комиссия Африканского союза

Конференция Black Hat USA

Конференция DEF CON

Представительство Европейского Союза в ООН в Женеве

Глобальный форум по вопросам киберпространства

Google

Муниципалитет Гааги

Packet Clearing House

Тель-Авивский университет

Институт Организации Объединенных Наций по исследованию проблем разоружения