Стратегия США в области международного киберпространства и цифровой политики

На пути к инновационному, безопасному и уважающему права цифровому будущему

Оглавление

Предисловие

Мы переживаем поворотный период международных отношений, характеризующийся острой конкуренцией между странами и общими глобальными вызовами, такими как изменение климата, продовольственная безопасность и безопасность в области здравоохранения, а также инклюзивный экономический рост.

Технологии будут играть все более важную роль в решении этих проблем. Именно поэтому в Государственном департаменте мы уделяем первоочередное внимание наращиванию потенциала и экспертных знаний в области кибербезопасности, цифровых технологий и новых технологий в рамках наших более широких усилий по модернизации дипломатии и обеспечению того, чтобы внешняя политика США соответствовала вопросам, наиболее важным для жизни и средств к существованию американского народа. В качестве ключевой вехи в этой работе я рад представить здесь Стратегию Департамента в области международного киберпространства и цифровой политики.

Центральное место в нашей стратегии занимают усилия по укреплению цифровой солидарности – совместная работа по оказанию взаимной помощи жертвам злонамеренной киберактивности и другого цифрового вреда; оказание помощи партнерам, особенно странам с формирующимся рынком, во внедрении безопасных, надежных, отказоустойчивых и устойчивых технологий для достижения их целей в области развития; и строит сильную и инклюзивную инновационную экономику, которая может определять наше экономическое и технологическое будущее. Мы объединяем коалиции правительств, бизнеса и гражданского общества, чтобы сформировать цифровую революцию на всех уровнях технологического «стека» — от строительства подводных кабелей и телекоммуникационных сетей до развертывания облачных сервисов и надежного искусственного интеллекта, а также продвижения управления данными с соблюдением прав человека и норм ответственного поведения государства.

Соединенные Штаты будут работать с любой страной или субъектом, которые привержены разработке и внедрению технологий, которые являются открытыми, безопасными и надежными, способствующими инклюзивному росту, способствующими устойчивому и демократическому обществу и расширяющими права и возможности всех людей.

Энтони Блинкен
Государственный секретарь

Введение

Соединенные Штаты стремятся работать с союзниками, партнерами и заинтересованными сторонами по всему миру, чтобы формировать дизайн, разработку, управление и использование киберпространства и цифровых технологий для содействия экономическому процветанию и инклюзивности; повышения безопасности и борьба с киберпреступностью; реализации и защиты прав человека, демократии и верховенства закона; и решения транснациональных проблем. Соединенные Штаты верят в важнейшую роль, которую ответственное использование цифровых технологий и взаимосвязанных сетей играет в расширении прав и возможностей людей, и в то, что открытый, функционально совместимый, безопасный и надежный интернет позволяет найти новые решения глобальных проблем. Однако автократические государства и другие субъекты используют кибер- и цифровые инструменты для того, чтобы угрожать международному миру и стабильности, причинять вред другим, оказывать злонамеренное влияние и подрывать осуществление прав человека. Инновационная, уважающая права человека стратегия политики в области международного киберпространства и цифровых технологий лежит в основе стратегических, экономических, внешнеполитических интересов США.

Лидерство в киберпространстве, цифровой экономике и новых цифровых технологиях имеет центральное значение для продвижения видения США, изложенного в Стратегии национальной безопасности (СНБ) от октября 2022 года, о «свободном, открытом, безопасном и процветающем мире». Являясь ведущим внешнеполитическим агентством Соединенных Штатов, Государственный департамент продвигает Национальную стратегию кибербезопасности (NCS) на 2023 год и ее цели по налаживанию международных партнерств для создания открытой, устойчивой, защищаемой и уважающей права человека цифровой экосистемы. Кроме того, она укрепляет двойной подход Стратегии: 1) перераспределение ответственности за защиту киберпространства на правительственные и частные организации, которые наиболее способны и находятся в наилучшем положении для снижения рисков, и 2) перераспределение стимулов для благоприятствования долгосрочным инвестициям в кибербезопасность посредством дипломатии, партнерства и обмена информацией. Эта стратегия будет дополнена готовящейся к выпуску Цифровой политикой Агентства США по международному развитию (USAID).

Для продвижения СНБ и НКС Государственный департамент в сотрудничестве с другими федеральными агентствами разработал стратегию международной политики в области киберпространства и цифровых

технологий, ориентированную на формирование широкой цифровой солидарности с помощью трех руководящих принципов и четырех областей действий, которые должны стать приоритетными в течение следующих трех-пяти лет.

Цифровая солидарность — это готовность работать вместе над достижением общих целей, помогать партнерам наращивать потенциал и оказывать взаимную поддержку. Цифровая солидарность признает, что все, кто использует цифровые технологии с уважением к правам человека, становятся более защищенными, устойчивыми, самоопределяющимися и процветающими, когда мы работаем вместе, чтобы формировать международную среду и внедрять инновации на технологическом переднем крае. Центральное место в принципах цифровой солидарности занимают усилия по оказанию поддержки союзникам и партнерам, особенно странам с формирующимся рынком, в стремлении в полной мере использовать возможности, предоставляемые новыми технологиями, и устойчиво добиваться своих целей в области экономики и развития. Цифровая солидарность согласовывает национальные интересы США с интересами наших международных партнеров с помощью совместимых подходов к управлению технологиями, поддерживает прочные партнерские отношения с гражданским обществом и частным сектором, а также обеспечивает устойчивость кибербезопасности, основанную на разнообразии продуктов и услуг, производимых надежными поставщиками технологий. В нем подчеркивается взаимная поддержка, которую Соединенные Штаты и их партнеры оказывают друг другу в противодействии злонамеренным кибероперациям, киберпреступности и другим цифровым угрозам и реагировании на них, а также поощряется совместные усилия государств и гражданских субъектов по защите и продвижению прав человека. Кроме того, концепция цифровой солидарности основывается на усилиях по наращиванию цифрового и киберпотенциала, с тем чтобы партнеры не только могли лучше строить защищенную и устойчивую цифровую экосистему в долгосрочной перспективе, но и могли быстро реагировать и восстанавливаться в случае инцидентов, угрожающих безопасности и правопорядку. Действия и усилия в рамках этой стратегии направлены на демонстрацию и укрепление цифровой солидарности с партнерами по всему миру.

Государственный департамент совместно с межведомственными партнерами будет выстраивать цифровую солидарность по четырем направлениям деятельности, фундаментально опираясь на три принципа:

- **Во-первых**, Государственный департамент будет придерживаться позитивного видения в отношении киберпространства и цифровых технологий,

ориентированного на предоставление преимуществ технологий и основанного на международных обязательствах и международном праве, включая международное право в области прав человека. Соединенные Штаты привержены сотрудничеству с союзниками и партнерами в целях создания будущего, в котором люди во всем мире будут безопасно использовать цифровые технологии для поиска, получения и распространения информации и идей в Интернете, участвуя в свободных, открытых и информированных обществах; доступ к образовательным и экономическим возможностям в целях стимулирования инклюзивного экономического роста; и надежно получать критически важные услуги и информацию от своих правительств.

- **Во-вторых**, Государственный департамент будет интегрировать кибербезопасность, устойчивое развитие и технологические инновации во все аспекты нашего подхода. Кибербезопасность, безопасность данных и киберустойчивость являются предпосылками и факторами экономического роста, и здоровыми гражданскими пространствами, где граждане могут осуществлять свои права; Страны не могут создать и поддерживать инновационную цифровую экосистему, приносящую пользу всем, не обеспечив ее сначала.
- **в-третьих**, Государственный департамент будет внедрять всеобъемлющий политический подход, использующий соответствующие инструменты дипломатии и международного государственного управления во всей цифровой экосистеме. Эта экосистема включает, помимо прочего, аппаратное обеспечение, программное обеспечение, протоколы, технические стандарты, поставщиков, операторов, пользователей и цепочки поставок, охватывающие телекоммуникационные сети, подводные кабели, облачные вычисления, центры обработки данных и инфраструктуру спутниковых сетей, операционные технологии, приложения, веб-платформы и потребительские технологии, а также Интернет вещей (IoT), искусственный интеллект (AI) и другие критически важные и новые технологии.

В соответствии с этими тремя принципами Государственный департамент будет выстраивать цифровую солидарность по четырем направлениям, которые вытекают из создания цифровых экосистем и управления ими, защиты от злонамеренных действий, оказания помощи и повышения устойчивости:

1. Продвигать, создавать и поддерживать открытую, инклюзивную, безопасную и устойчивую цифровую экосистему;
2. Согласование с международными партнерами подходов к цифровому управлению и управлению данными, основанных на уважении прав человека;

3. Поощрение ответственного поведения государств в киберпространстве и противодействие угрозам киберпространству и критически важной инфраструктуре путем создания коалиций и привлечения партнеров;

4. Укреплять и наращивать цифровой и кибернетический потенциал международных партнеров.

Государственный департамент будет укреплять усилия по формированию цифровой солидарности путем активного участия в международных, многосторонних и многосторонних органах, где разрабатываются обязательства, нормы, стандарты и принципы, влияющие на вопросы киберпространства, цифровых технологий, интернета и технологий. В то время как прогресс в этих сферах может быть медленным и постепенным (часто в зависимости от их целей), отсутствие лидерства США на международных форумах может позволить противникам заполнить пустоту и сформировать будущее технологий в ущерб интересам и ценностям США.

Почти все вопросы внешней политики – от международной безопасности до демократии и прав человека, глобального здравоохранения и изменения климата – будут определяться сегодняшними инвестициями в киберпространство и дипломатию цифровых технологий. Государственный департамент будет руководить межведомственным процессом по установлению, координации и интеграции усилий в области кибердипломатии и цифровых технологий для продвижения национальных интересов и ценностей США в течение следующего десятилетия и далее. Однако эффективность усилий США и связанных с ними посланий частично зависит от последовательности и действий внутри страны, как в политике, так и в ее исполнении. Например, американские технологические компании являются лидерами первой волны цифровизации и в настоящее время продвигают инновационные технологии в области систем искусственного интеллекта. Таким образом, Соединенные Штаты должны быть лидером в продвижении ответственности за технологические платформы. Мы должны помочь возглавить ответственное проектирование, разработку, управление и использование технологий следующей волны в соответствии с демократическими ценностями и уважением прав человека.

У Соединенных Штатов есть сильные стороны, которые служат нам в формировании будущего цифровых технологий: прочные альянсы и партнерства; самые инновационные технологические компании мира; прозрачная, инклюзивная и благоприятная политическая среда; а также активное и активное гражданское общество, и технические сообщества. Соединенные Штаты мобилизуют эти ресурсы для реализации этой

позитивной и упреждающей международной стратегии в киберпространстве и цифровом пространстве.

Цифровой мир: возможности и вызовы

Цифровые технологии произвели революцию в том, как мы живем, работаем и учимся. Они, наряду с расширением возможностей взаимосвязанности, не только стимулируют экономический рост, но и способствуют осуществлению прав человека и улучшают доступ к образованию, финансовым и социальным услугам. Цифровые технологии создали новые рынки и возможности, а также позволили предприятиям охватить обширную клиентскую базу за пределами своей страны. Новые цифровые инструменты активизировали гражданскую и политическую активность, демократизировали информацию и знания, использовались для обеспечения подотчетности правительств и компаний, а также повысили прозрачность, эффективность и оперативность государственных услуг.

Заглядывая в будущее, можно сказать, что эти технологии могут открыть беспрецедентные возможности для решения некоторых из наиболее насущных глобальных проблем, включая изменение климата, экономическое и социальное неравенство и кризисы в области здравоохранения. Используя возможности анализа данных, искусственного интеллекта и связи в режиме реального времени, мы можем создавать более умные и устойчивые города, повышать урожайность сельскохозяйственных культур с меньшими затратами ресурсов и делать здравоохранение доступным даже для самых отдаленных населенных пунктов. Эти технологии позволяют разрабатывать решения в области «зеленой» энергетики, способствуя переходу к более чистой и менее дорогой энергии. Достижения в области сбора, моделирования, симуляции и анализа данных позволят ученым ускорить исследования и открытия, а также выявлять закономерности, невидимые только для человека, катализируя быстрые и неожиданные прорывы. Объединяя людей и информацию, как никогда раньше, цифровые технологии могут способствовать построению более инклюзивного и справедливого мира, в котором возможности для процветания и благополучия имеются в изобилии для всех.

В то же время стремительное распространение и эволюция цифровых технологий наносят значительный вред. Геополитика киберпространства конкурентна и сложна. Злонамеренные государственные и негосударственные субъекты развили возможности и продемонстрировали намерение подвергнуть риску критически важную инфраструктуру, национальные критически важные функции и даже отдельных граждан. Авторитарные государства продвигают

конкурирующие формы управления технологиями, которые используют массовую слежку, практику сбора данных, нарушающую неприкосновенность частной жизни, и инструменты онлайн-цензуры, которые угрожают открытому, функционально совместимому, безопасному и надежному Интернету. Технологии предоставляют новые векторы и инструменты для преступности, а резкое распространение личной информации в Интернете расширило среду угроз. Распространение и неправомерное использование коммерческих шпионских программ представляет угрозу национальной безопасности, нацеленную на должностных лиц США за рубежом; Коммерческое шпионское ПО также использовалось для того, чтобы нацеливаться на предполагаемых оппонентов и запугивать их, способствовать усилиям по обузданию инакомыслия и, таким образом, подрывать демократические ценности. Журналисты, активисты, педагоги, исследователи, женщины и девочки, а также маргинализированные группы часто становятся жертвами незаконной слежки, онлайн-преследований и злоупотреблений. Каждая страна и каждая из технологических платформ должны сыграть свою роль в смягчении алгоритмической предвзятости и манипулирования информацией, а также насильственных экстремистских сообщений, материалов о сексуальном насилии над детьми (CSAM), гендерного насилия с использованием технологий и другого вредоносного контента.

Эти вызовы являются насущными и требуют высоких ставок. Инновации, партнерство, сотрудничество, создание коалиций, обмен информацией, взаимная поддержка, помощь и другие инструменты дипломатии имеют важнейшее значение для обеспечения того, чтобы цифровые технологии защищали и продвигали индивидуальную свободу и способствовали экономическому процветанию.

Кибератаки и угрозы национальной безопасности

Враждебные киберкампании могут в совокупности привести к стратегическим потерям для Соединенных Штатов и их союзников, и они все больше ставят под угрозу цели развития развивающихся экономик. Киберугрозы продолжают усиливаться как по частоте, так и по серьезности, при этом возрастают риски эскалации или неконтролируемой киберактивности. Государственные и негосударственные субъекты, в том числе преступники, террористы и воинствующие экстремисты, имеют огромные стимулы инвестировать в цифровые технологии и использовать их для того, чтобы угрожать нашим национальным интересам и национальным интересам других стран.

Китайская Народная Республика (КНР) представляет собой самую широкую, самую активную и наиболее устойчивую киберугрозу для сетей государственного и частного секторов в Соединенных Штатах. Пекин организовал операции кибершпионажа против правительственных, коммерческих и гражданских структур и расширил свои возможности по осуществлению деструктивных и подрывных кибератак. КНР способна проводить кибератаки, которые могут нарушить работу нефте- и газопроводов, железнодорожных систем и других критически важных инфраструктурных служб на территории Соединенных Штатов или их союзников и партнеров. Попытки КНР скомпрометировать критически важную инфраструктуру отчасти направлены на то, чтобы заранее подготовиться к тому, чтобы иметь возможность нарушить или уничтожить критически важную инфраструктуру в случае конфликта — либо для того, чтобы помешать Соединенным Штатам проецировать силу в Азию, либо для того, чтобы повлиять на процесс принятия решений во время кризиса, спровоцировав социальный хаос внутри Соединенных Штатов. Как спонсируемая государством деятельность, так и деятельность, связанная с КНР, является частью киберподхода КНР.

Будучи постоянной киберугрозой, российское правительство совершенствует свои возможности кибершпионажа, кибератак, влияния и манипулирования информацией, чтобы угрожать другим государствам и ослаблять альянсы и партнерства США. Россия продолжает предоставлять убежище транснациональным киберпреступникам, таким как банды вымогателей. Кибератаки России в поддержку ее неспровоцированного вторжения в Украину в 2022 году были направлены на дестабилизацию украинского государства и вооруженных сил и привели к побочным эффектам на гражданскую критическую инфраструктуру в других европейских странах. По мере того, как война продолжается, российское правительство и связанные с ним киберсубъекты нацеливаются на Украину с помощью кибероперaций против государственного и частного секторов, манипулирования информацией и онлайн-влияния, а также попыток отвлечь и подвергнуть цензуре доступ украинцев к интернету. Россия, судя по всему, уделяет особое внимание улучшению своей способности наносить удары по критически важной инфраструктуре в Соединенных Штатах, чтобы продемонстрировать свою способность наносить ущерб инфраструктуре во время кризиса.

Правительства Северокорейской Народно-Демократической Республики (КНДР) и Ирана увеличили масштабы своей злонамеренной кибердеятельности. Столкнувшись с многочисленными раундами международных санкций, КНДР уклоняется от контроля с помощью киберпреступности и кражи криптовалют. Хакеры КНДР продолжают

собирать разведданные о военных технологических объектах, а также о научных кругах и аналитических центрах. Кроме того, КНДР отправляет тысячи квалифицированных ИТ-специалистов по всему миру для получения мошеннических доходов, которые в конечном итоге способствуют ее программам по созданию оружия массового уничтожения и баллистических ракет, несмотря на санкции США и ООН.

Растущий опыт Ирана и его готовность проводить кибероперации угрожают безопасности сетей и данных во всем мире. Оппортунистический подход Ирана к кибератакам делает владельцев критически важной инфраструктуры в Соединенных Штатах уязвимыми для иранских субъектов, особенно когда Тегеран считает, что он должен продемонстрировать, что он может дать отпор Соединенным Штатам в других областях. Иранские субъекты участвовали в широком спектре операций по сбору разведданных по всему миру, а после зверств ХАМАСа 7 октября 2023 года и военных операций Израиля в Газе проводили операции по удалению веб-сайтов, взлому и утечке информации, шпионажу и кампаниям по манипулированию информацией в Интернете. Иранские субъекты также ведут злонамеренную деятельность против устройств операционных технологий, используемых в водном секторе и других отраслях промышленности.

Киберпреступники и преступные синдикаты, действующие в киберпространстве, в настоящее время представляют особую угрозу экономической и национальной безопасности стран по всему миру. Киберпреступность и онлайн-мошенничество наносят значительный ущерб экономическому развитию, при этом малые и средние предприятия и поставщики финансовых услуг подвергаются особому риску. По некоторым оценкам, в 2027 году глобальный ущерб от киберпреступности превысит 23 триллиона долларов.

Инциденты, связанные с программами-вымогателями, нарушили работу критически важных функций, служб и предприятий, от энергетических трубопроводов и продовольственных компаний до школ и больниц. Атаки программ-вымогателей на отрасль здравоохранения могут подорвать уровень медицинской помощи, оказываемой пациентам и другим лицам, находящимся под наблюдением. Общий экономический ущерб от атак программ-вымогателей во всем мире продолжает расти, достигая миллиардов долларов США ежегодно. Группы вымогателей часто действуют из юрисдикций-убежищ, правительства которых, часто такие противники, как Россия, не сотрудничают с правоохранительными органами, а иногда поощряют, направляют, наказывают или терпят их деятельность.

Использование террористами и воинствующими экстремистами цифровых технологий также представляет угрозу национальной безопасности Соединенных Штатов и их союзников и партнеров. Злонамеренная деятельность включает использование информационно-коммуникационных технологий (ИКТ) для распространения пропаганды насилия; поощрять радикализацию и мобилизацию для совершения насильственных действий; вербовка отдельных лиц в террористические организации; тренировать, планировать и координировать атаки; и финансировать террористические акты.

Конкурирующие нормы Интернета

Россия, КНР и другие авторитарные государства продвигают концепцию глобального управления интернетом, которая сосредоточена на внутреннем контроле и нисходящих, государственно-центричных механизмах над существующими процессами с участием многих заинтересованных сторон по принципу «снизу-вверх». Россия и КНР пытаются использовать многосторонние форумы, такие как ООН, для оказания влияния на развивающиеся страны и обращения к ним с целью перекроить глобальный ландшафт кибер- и технологической политики для продвижения авторитарной повестки дня, одновременно мешая Соединенным Штатам и их союзникам. Россия, КНР и другие страны стремятся изменить нормы, регулирующие киберпространство, подорвать техническую основу интернета и ослабить ответственность за злонамеренное использование возможностей киберпространства авторитарными странами.

Авторитарные правительства работают над тем, чтобы ослабить глобальную приверженность универсальным правам человека, закрепленным во Всеобщей декларации прав человека и международно-правовых документах, таких как Устав ООН и Международный пакт о гражданских и политических правах. Авторитарные правительства, в первую очередь КНР, активно работают над тем, чтобы кооптировать и переосмыслить устоявшуюся терминологию, связанную с «демократией» и «правами человека», в контексте разработки международной политики в области технологий, в том числе посредством своего вклада в процесс «Пакт о будущем» ООН и его Глобальный цифровой договор.

Угрозы интернету и цифровой свободе

Авторитарные и нелиберальные государства стремятся ограничить права человека в Интернете и за его пределами, злоупотребляя интернетом и

цифровыми технологиями. Правительства закрывают и изолируют Интернет: подавляют инакомыслие с помощью отключений Интернета и телекоммуникаций, виртуальных отключений, ограниченных сетей и блокировки веб-сайтов.

КНР разработала масштабную систему слежки, и ее фирмы в настоящее время экспортируют свой подход к регулированию и технические возможности, чтобы облегчить контроль и репрессии других правительств. Пекин также использует киберсредства для нападения на людей за пределами своих границ, включая журналистов, диссидентов и отдельных лиц, которых он считает угрозой нарративам, политике и действиям Коммунистической партии Китая. После полномасштабного вторжения в Украину в 2022 году российское правительство заблокировало доступ к иностранным сайтам и усилило цензуру и слежку за отечественными пользователями. Иранское правительство продолжает полагаться на интернет-ограничения, фильтрацию и слежку для подавления оппозиции режиму.

Все большее число правительств, в том числе отстающих демократий, злоупотребляют цифровыми инструментами таким образом, что нарушают или злоупотребляют правом человека на свободу от произвольного или незаконного вмешательства в частную жизнь, а также ограничивают и угрожают правам людей на свободу выражения мнений, ассоциаций и мирных собраний. Коммерческое шпионское ПО, программное обеспечение для распознавания лиц с поддержкой искусственного интеллекта и другие технологии слежки неправомерно используются против журналистов, правозащитников и других активистов, женщин и членов маргинализированных групп, в том числе за пределами стран. Гендерное насилие с использованием технологий ограничивает свободу слова, препятствует неприкосновенности частной жизни и свободе выражения мнений, а также подрывает способность женщин, девочек и представителей ЛГБТКИ+ участвовать в демократии, управлении и гражданской жизни.

Распространение онлайн-манипуляций в сочетании с угрозами, исходящими от иностранных противников, стремящихся вмешаться в целостность информации, представляет собой фундаментальную угрозу демократии, подрывая доверие к институтам, угрожая избирательным процессам и сея раздор внутри стран и между ними. Субъекты КНР расширили свои возможности по проведению тайных операций влияния и распространению дезинформации. Даже если Пекин установит ограничения на эту деятельность, лица, не находящиеся под его непосредственным контролем, могут попытаться повлиять на выборы, которые, по их мнению, соответствуют целям КНР. Российское правительство остается серьезной угрозой

иностранного влияния из-за его широкомасштабных усилий, направленных на то, чтобы попытаться расколоть западные альянсы и подорвать позиции США в мире. В последнее время российские субъекты влияния адаптировали свои усилия для того, чтобы лучше скрывать свою руку.

Вызовы цифровой экономики

Около 2,6 миллиарда человек до сих пор не имеют доступа к интернету, в результате чего треть населения мира не имеет доступа к интернету. Эта ситуация представляет собой вызов экономическому развитию для многих стран и стратегический вызов для Соединенных Штатов и их союзников, и партнеров. Оставленный без внимания, цифровой разрыв не только ставит под угрозу усилия по созданию прочной цифровой экосистемы, но и угрожает ростом неравенства доходов и нестабильности в странах с формирующимся рынком. Цифровой разрыв непропорционально сильно затрагивает женщин и другие маргинализированные группы. Например, 80 процентов женщин в странах с низким уровнем дохода не пользуются интернетом.

По мере того, как мир становится все более цифровым, страны по всему миру пытаются найти подход к цифровой экономике таким образом, чтобы воспользоваться ее преимуществами, устранить ее риски и расширить ее охват для большего числа людей. Правительства разрабатывают различные подходы к регулированию по целому ряду политических вопросов, таких как защита безопасности, здоровья и неприкосновенности частной жизни детей, борьба с TFGBV, борьба с антиконкурентным поведением, обеспечение равного доступа к соединениям и технологиям, создание надежной цифровой инфраструктуры и содействие надежным трансграничным потокам данных.

Все большее число стран продвигают цифровую общественную инфраструктуру (DPI) как важнейшую составляющую экономического роста, надлежащего управления и достижения целей устойчивого развития (ЦУР) ООН. Определение DPI постоянно меняется, но в целом включает в себя сетевые стандарты открытых технологий, разработанные в общественных интересах, благоприятную нормативно-правовую среду и сообщество участников рынка, движущих инновации. Несмотря на то, что некоторые из наиболее известных моделей включают в себя цифровую идентификацию, цифровые платежи и платформы данных для обмена и хранения данных, универсального решения не существует. Модели DPI должны основываться на гарантиях, включая защиту прав человека, и такие модели должны быть функционально совместимыми.

Правительство США и представители частного сектора стремятся использовать данные и цифровую экономику для получения положительных экономических и социальных выгод: сохранения открытости при одновременной защите конфиденциальности, обеспечения безопасности и смягчения ущерба. Государственный департамент США, работая с другими агентствами, стремится формировать рынки и защищать инновации от регуляторных эксцессов. Несмотря на то, что некоторые страны проявляют все большую готовность поддерживать нарративы о цифровом суверенитете и протекционизме, блокируя доступ к своим рынкам, неправомерно препятствуя трансграничным потокам данных и отдавая предпочтение отечественным производителям и поставщикам услуг, мы продолжаем международное взаимодействие в целях повышения функциональной совместимости, безопасности и доступа к рынкам.

Многие государства продвигают цифровые технологии для экономического роста, пытаясь при этом сохранить автономию и нейтралитет. Они стремятся быстро и дешево создать цифровую инфраструктуру и ищут помощи в борьбе с киберпреступностью и развитии потенциала кибербезопасности. Тем не менее, правительство КНР искажает рынки, чтобы получить выгоду от поставщиков оборудования, программного обеспечения и услуг в КНР, что ставит под угрозу безопасность клиентов. Соединенные Штаты, напротив, стремятся предоставить странам с формирующимся рынком и развивающимся странам финансово обоснованные альтернативы неустойчивым инициативам. Государственный департамент привержен сотрудничеству с союзниками и партнерами в целях предложения и развертывания безопасных технологий, которые позволяют странам и гражданским субъектам по всему миру создавать цифровую инфраструктуру и повышать кибербезопасность во всех секторах, принося непосредственные выгоды правительствам и помогая обеспечить защиту прав человека и неприкосновенности частной жизни своих граждан, что позволит создать инклюзивную цифровую экономику.

Будущее управления технологиями искусственного интеллекта

Неопределенность и сложность, характеризующие геополитическое соперничество за эти цифровые технологии, усугубляются тем фактом, что мы стоим на пороге очередной технологической революции. Революция в системах искусственного интеллекта может произойти даже более быстрыми темпами, чем развитие и внедрение Интернета. Технологии ИИ могут стать мощными инструментами для расширения знаний, повышения благосостояния

и производительности, а также решения глобальных проблем, а инструменты ИИ могут способствовать достижению семнадцати ЦУР ООН. Приложения ИИ обладают дальнейшим потенциалом для улучшения многих аспектов жизни граждан, включая продовольственную безопасность, приложения в области здравоохранения, надлежащее управление и демократическую консолидацию, а также готовность к стихийным бедствиям и их предотвращение.

Однако быстрое развитие технологии ИИ сопряжено со значительным риском того, что ее использование может усугубить неравенство и экономическую нестабильность, подавить конкуренцию, причинить вред потребителям, усугубить дискриминацию и предвзятость, вторгнуться в частную жизнь, усилить злонамеренную киберактивность и улучшить авторитарные возможности для слежки и репрессий. Искусственный интеллект будет оспаривать то, как мы компенсируем использование интеллектуальной собственности, а также аутентифицируем, маркируем или обнаруживаем синтетический контент. Кроме того, ИИ может потребовать адаптации рабочей силы в разных странах; растущие потребности в энергии для высокотехнологичных микросхем искусственного интеллекта и центров обработки данных могут стать серьезным препятствием для развития локальных возможностей.

Кроме того, было замечено, что государственные и негосударственные субъекты используют системы генеративного ИИ в злонамеренных целях, в том числе для манипулирования и распространения дезинформации с высокой скоростью и в больших масштабах. Кроме того, многие технологии ИИ имеют двойное назначение, что позволяет создавать новые военные возможности и средства национальной безопасности, в которых могут отсутствовать надлежащие меры защиты прав человека и гражданских свобод и других гарантий. Искусственный интеллект может принести пользу как злоумышленнику, так и обороняющемуся в киберпространстве, а сами системы подвержены отравлению данных и другим видам вредоносных действий.

Вопрос о том, как сбалансировать риск и вознаграждение, стоит перед правительствами и гражданским обществом во всем мире. Соединенные Штаты работают с союзниками и партнерами, чтобы быстро решить проблемы, с помощью которых искусственный интеллект потенциально может дестабилизировать общество, сохраняя при этом свои преимущества и, что особенно важно, оставаясь верными демократическим ценностям и защищая права человека. Важнейшей частью этой работы является не только обеспечение открытой и независимой исследовательской среды, но и партнерство с развивающимися экономиками в области разработки и внедрения технологий ИИ. Оказание помощи в обеспечении неограниченного

доступа к открытому, функционально совместимому, надежному и безопасному интернету при одновременной демонстрации того, как ИИ может служить общей повестке дня во всем мире, может помочь снизить риск того, что революция ИИ будет способствовать глобальной нестабильности и уменьшит нашу способность решать глобальные проблемы.

Работа с частным сектором и гражданским обществом

Конкуренция, потребительский выбор, динамичные инвестиции частного сектора и активное гражданское общество являются отличительными чертами открытой, инклюзивной и безопасной цифровой экосистемы. Государственный департамент не может достичь своих целей без прочных партнерских отношений с частным сектором, гражданским обществом, академическими и техническими сообществами. Новые инновации исходят из частного сектора, и решения, принимаемые технологическими компаниями о том, как разрабатывать и развертывать свои системы, имеют глубокие последствия для того, как реализуются ценности и интересы США, включая защиту безопасности и конфиденциальности пользователей. Официальные лица США полагаются на ряд представителей частного сектора, академических кругов и гражданских структур для понимания технологических разработок, а заинтересованные стороны из частного сектора и торговых ассоциаций часто обеспечивают раннее предупреждение о дискриминационных правилах, которые явно направлены против американских компаний. Надежные поставщики технологий, в том числе малые и средние предприятия, являются важными партнерами в усилиях по расширению возможностей подключения с помощью открытых, безопасных и отказоустойчивых сетей по всему миру.

Группы гражданского общества работают над тем, чтобы люди могли получить доступ к возможностям в Интернете, свободным от незаконной слежки и практики сбора данных, нарушающей неприкосновенность частной жизни, и работают над противодействием вредной пропаганде и дезинформации в цифровом пространстве. Гражданское общество и техническое сообщество часто первыми распознают, предупреждают и ищут решения для угроз правам человека в Интернете и за его пределами. По мере того, как свобода интернета продолжает снижаться в некоторых частях мира, активисты гражданского общества, правозащитники и журналисты, освещающие их деятельность, часто возглавляют сопротивление в репрессивных обществах с цифровыми технологиями, часто с большим риском для себя. Кроме того, гражданское общество, научное и техническое сообщество, а также представители частного сектора играют решающую роль в

поддержании многосторонней модели управления интернетом, которая находится под растущей угрозой.

Частный сектор, гражданское общество и техническое сообщество играют важнейшую роль в защите от злонамеренной кибердеятельности. В 2022 году частный сектор помогал Албании после иранских кибератак, а во время полномасштабного вторжения России в Украину технологические фирмы и компании по кибербезопасности предоставляли услуги, инструменты и информацию об угрозах, чтобы помочь Украине защитить правительственные сети и сети критической инфраструктуры. Они перенесли услуги хранения данных и облачного хостинга, чтобы противодействовать попыткам России стереть критически важные данные, а также предоставляли интернет и телекоммуникационные услуги, которые помогали поддерживать работу государственных учреждений и бизнеса. Неправительственные организации и научно-исследовательские группы разоблачили угрозу, исходящую от распространения и неправомерного использования коммерческих шпионских программ против журналистов, активистов и маргинализированных групп.

Государственно-частные партнерства имеют важнейшее значение для кибер- и цифровой дипломатии, и они должны быть гибкими и адаптируемыми. Киберзащита может потребовать новых способов масштабирования, поставки и лицензирования услуг и продуктов киберзащиты в условиях кризиса, и ее может быть трудно запустить и поддерживать в другом региональном контексте. Репрессивные правительства разрабатывают новые методы контроля над цифровыми технологиями, манипулирования информационными потоками и вмешательства в них. Для решения этих и других возникающих проблем Государственный департамент будет продолжать расширять контакты с широким кругом представителей гражданского общества и частного сектора и запрашивать их вклад. Кроме того, Соединенные Штаты продолжат работать с союзниками и партнерами над продвижением многостороннего подхода к цифровому управлению и управлению данными.

Укрепление цифровой солидарности

Соединенные Штаты считают, что цифровые технологии могут и должны использоваться для того, чтобы направить людей на путь процветания, решения глобальных проблем и построения лучшего будущего для всех. Государственный департамент будет работать с союзниками, партнерами и заинтересованными сторонами над продвижением позитивного видения кибер-

и цифровых технологий: такого, в рамках которого люди во всем мире используют киберпространство и цифровые технологии для содействия экономическому процветанию и инклюзивности; повышение безопасности и борьба с киберпреступностью; поощрение и защита прав человека, гендерного равенства, демократии и верховенства закона; и решать транснациональные проблемы. В рамках этого подхода Соединенные Штаты, их союзники и партнеры продемонстрируют преимущества открытого, функционально совместимого, безопасного и надежного интернета; выступать в качестве предпочтительного партнера в области исследований, проектирования, разработки и внедрения цифровых и новых технологий; и совместно налагать последствия за поведение, противоречащее международно признанным нормам поведения государств. Государственный департамент также будет работать и поддерживать усилия стран с развивающейся экономикой по улучшению кибербезопасности и повышению их киберустойчивости.

Каждое из четырех направлений деятельности Стратегии: продвижение, создание и поддержание открытой, инклюзивной, безопасной и устойчивой цифровой экосистемы; согласование правозащитных подходов к цифровому управлению; продвигать ответственное поведение государства, противодействовать злонамеренной деятельности и оказывать взаимную поддержку; а также укрепление помощи в наращивании цифрового и кибернетического потенциала, что отражает аспекты видения Государственного департамента цифровой солидарности. В дальнейшем Государственный департамент будет работать над привлечением широкого круга партнеров по всему миру к процессу формирования и расширения цифровой солидарности. Мы приветствуем всех тех, кто стремится разрабатывать и внедрять открытые и безопасные технологии, содействовать инклюзивному росту, укреплять жизнестойкие и демократические общества и расширять права и возможности всех, включая наиболее уязвимые слои населения.

НАПРАВЛЕНИЕ ДЕЯТЕЛЬНОСТИ 1: Продвигать, создавать и поддерживать открытую, инклюзивную, безопасную и устойчивую цифровую экосистему

Цифровая солидарность опирается на инновации в рамках открытой, инклюзивной, безопасной и устойчивой цифровой экосистемы и подкрепляется ими. Несмотря на то, что Соединенные Штаты являются крупной державой в области цифровых, критически важных и новых технологий, мы не можем и не должны действовать в одиночку. Напротив, Соединенные Штаты, их союзники

и партнеры становятся более процветающими, самоопределяющимися и устойчивыми, когда мы работаем вместе, чтобы катализировать, поддерживать и поддерживать быстрое технологическое развитие по целому ряду критически важных технологий.

В тесной координации с союзниками, партнерами, частным сектором и гражданским обществом Государственный департамент продолжает кампанию за открытые, функционально совместимые, безопасные, надежные и надежные телекоммуникационные сети, особенно в беспроводных сетях пятого поколения (5G). Белый дом, Государственный департамент, USAID, Министерство торговли и Федеральная комиссия по связи (FCC) ведут переговоры с союзниками и партнерами о развертывании мобильных сетей 5G с использованием надежных поставщиков и будущем 6G. Цифровые технологии не ограничиваются беспроводными технологиями, и Государственный департамент и другие ведомства координируют свои действия с союзниками и партнерами по разработке, развертыванию и обеспечению безопасности облачной инфраструктуры и центров обработки данных, подводных кабелей и спутниковой связи. Кроме того, во всех органах ООН Соединенные Штаты стремятся содействовать на высоком уровне разработке, внедрению и использованию цифровых технологий, уважающих права человека.

Направление усилий 1: Содействие разработке и внедрению открытых, инклюзивных, безопасных и отказоустойчивых сетей электросвязи

Приложения 5G быстро развиваются, расширяя возможности цифровой связи новыми способами и создавая новые уязвимости кибербезопасности. Телекоммуникационные сети должны строиться с использованием продуктов надежных поставщиков, которые работают и имеют партнеров по цепочке поставок, которые действуют, прежде всего, в странах, которые уважают права путем последовательного применения закона через независимую судебную систему, в соответствии с принципами, отраженными в Декларации Организации экономического сотрудничества и развития (ОЭСР) о доступе правительств к персональным данным, находящимся в распоряжении организаций частного сектора. Телекоммуникационные сети не должны строиться с использованием продукции поставщиков, находящихся под контролем или влиянием авторитарного режима, и без значимых, независимых сдержек и противовесов или судебной защиты от требований правительства. Международные принципы, связанные с 5G, такие как Пражские предложения по безопасности 5G и Пражские предложения по разнообразию поставщиков телекоммуникационных услуг, поддерживают рыночную

конкурентоспособность и разнообразие надежных поставщиков оборудования 5G.

Эти усилия также распространяются на компонент «Цифровая инфраструктура» Партнерства в интересах глобальной инфраструктуры и инвестиций. Признавая, что стоимость часто является основным движущим фактором при закупках ИКТ, Соединенные Штаты оказывают поддержку правительствам, поставщикам интернет-инфраструктуры среднего звена и поставщикам интернет-услуг в развитии большей конкуренции и разнообразия в цепочках поставок электросвязи, в частности, в рамках Партнерства по цифровым соединениям и кибербезопасности (DCCP). DCCP – это общеправительственная инициатива, возглавляемая Государственным департаментом, направленная на наращивание потенциала, техническую помощь, а также разработку и финансирование проектов в поддержку открытого интернета и повышения кибербезопасности.

Кроме того, в соответствии с Законом о чипах и науке было выделено 500 миллионов долларов США в Международный фонд технологической безопасности и инноваций (ITSI) для Государственного департамента для поддержки разработки и внедрения безопасных цепочек поставок полупроводников и телекоммуникационных сетей. Соединенные Штаты будут использовать это финансирование для продолжения работы с партнерами в целях создания политических и нормативных рамок для безопасных экосистем ИКТ и создания равных условий для безопасных и заслуживающих доверия поставщиков.

Наряду с помощью в создании безопасных сетей, цифровая солидарность также выражается в усилиях по созданию цифровой инфраструктуры, которая способствует конкуренции, расширяет потребительский выбор и возлагает на сообщества и отдельных лиц ответственность за свою цифровую жизнь и ресурсы. Признавая необходимость привлечения капитала и снижения рисков потенциальных инвестиций в цифровую инфраструктуру, USAID при финансировании DCCP запустило программу смешанного финансирования под названием Digital Invest, которая сотрудничает с управляющими фондами и разработчиками проектов для расширения доступа к интернету и цифровым финансовым услугам на развивающихся рынках по всему миру. На сегодняшний день 13 партнеров Digital Invest привлекли первоначальные 8,45 млн долларов США из финансирования Государственного департамента и USAID для привлечения более 300 млн долларов США инвестиционного капитала для поставщиков цифровых финансов и интернет-услуг на развивающихся рынках, которые используют защищенное сетевое

оборудование, что стало катализатором дополнительного финансирования в размере 1,15 млрд долларов США от сторонних инвесторов.

Программы помощи иностранным государствам США также усилят конкуренцию на рынке и будут способствовать разнообразию поставщиков телекоммуникационных услуг за счет развития открытых и функционально совместимых интерфейсов и протоколов, таких как открытые сети радиодоступа (Open RAN). Такая открытая сетевая архитектура упрощает выход на рынок новых поставщиков, снижает затраты на развертывание и ускоряет внедрение инноваций. Open RAN предоставляет развивающимся странам возможность напрямую участвовать в цепочке поставок, например, через локальную сборку и разработку программного обеспечения. Не менее важно и то, что Open RAN предлагает альтернативы для использования технологий от ненадежных поставщиков. В результате, Государственный департамент будет продолжать поддерживать такие усилия, как финансирование коммерческих испытаний, технико-экономических обоснований, реверсивных торговых миссий, а также мероприятия по обучению и повышению осведомленности рабочей силы, которые продвигают Open RAN. Соединенные Штаты продолжат сотрудничество с правительствами Австралии, Канады, Японии и Соединенного Королевства по вопросам диверсификации цепочек поставок телекоммуникаций и связанных с этим вопросов в рамках Глобальной коалиции по электросвязи, созданной в октябре 2023 года.

Работая с правительствами других стран и частным сектором, Соединенные Штаты также готовятся к новой волне инноваций. В течение следующего десятилетия 6G обеспечит еще более высокие скорости, большую пропускную способность и меньшую задержку беспроводной связи. Встраивание открытых и функционально совместимых сетевых архитектур, таких как Open RAN, в разработку 6G с самого начала поможет обеспечить разнообразие поставщиков и устойчивость цепочки поставок. В феврале 2024 года Соединенные Штаты вместе с Австралией, Канадой, Чешской Республикой, Финляндией, Францией, Японией, Республикой Корея, Швецией и Великобританией одобрили общие принципы исследований и разработок систем беспроводной связи 6G.

Направление усилий 2: Дальнейшее достижение общего понимания и общих принципов безопасного использования и надежности облачных сервисов, центров обработки данных и связанных с ними инфраструктурных технологий

Облачные вычисления стали важным фактором цифровой трансформации экономики и бизнеса. Предоставляя доступ по требованию к масштабируемым вычислительным ресурсам надежным и экономичным способом, облачные сервисы позволяют государственным учреждениям и предприятиям предоставлять более безопасные и отказоустойчивые услуги своим гражданам и клиентам. Более того, облачные сервисы оказались стратегическим активом, поскольку российские войска физически уничтожили украинские объекты, на которых хранились критически важные данные. Миграция правительственной ИТ-инфраструктуры в облако повысила устойчивость и сохранила информацию, необходимую для функционирования экономики и правительства.

Американские компании, занимающиеся облачными вычислениями и центрами обработки данных, конкурируют по всему миру и предлагают услуги широкой международной клиентской базе, в то время как правительство Соединенных Штатов активно сотрудничает с иностранными правительствами для содействия справедливому и безопасному использованию ресурсов облачных вычислений. В то же время провайдеры из авторитарных государств глобализируются, и они часто более чутко реагируют на краткосрочные цели местного экономического развития, предоставляя пакеты, включающие финансовые субсидии, локальную облачную инфраструктуру и обучение рабочей силы. Облачные сервисы и центры обработки данных также являются источником напряженности в отношениях с близкими торговыми партнерами. Некоторые из них пригрозили исключить американских поставщиков облачных услуг со своих рынков отчасти из-за опасений по поводу доступа к данным и контроля над ними, несмотря на то, что Закон США «О разъяснении законного использования данных за рубежом» (CLOUD) предусматривает соглашения, обеспечивающие последовательную защиту на основе верховенства закона. Государственный департамент стремится достичь взаимопонимания с нашими международными партнерами по вопросам справедливого и безопасного использования ресурсов облачных вычислений.

Кроме того, Государственный департамент будет работать с международными партнерами и частным сектором над устранением расходов и увеличением поддержки создания безопасной облачной инфраструктуры в странах с развивающейся экономикой. DCCP усиливает эти усилия, поддерживая технико-экономические обоснования, обратные торговые миссии, финансирование и программы обучения, такие как гранты на обучение на Филиппинах для поддержки предоставления возможностей облачных вычислений.

Направление усилий 3: Повышение безопасности и упругости подводных кабелей

По подводным кабелям проходит более 95 процентов мирового цифрового трафика. По мере того, как данные продолжают распространяться и увеличиваться в геометрической прогрессии, растет и спрос на кабели и другие системы передачи. Обрыв или разрушение кабелей в результате аварий, стихийных бедствий или злонамеренных действий может привести к изоляции округа, угрозе национальной безопасности и нанести ущерб экономике на миллиарды долларов. Выбор поставщиков для подводной кабельной инфраструктуры, технического обслуживания и ремонта может либо стимулировать развитие и инновации, либо привести к новым формам зависимости и незащищенности. В связи с этим Государственный департамент в координации с другими ведомствами будет уделять первоочередное внимание повышению безопасности и устойчивости подводных кабелей.

Американские фирмы и другие надежные поставщики являются ведущими производителями многих сетевых компонентов, встроенных технологий и сопутствующих услуг для подводных кабелей, а также инвестируют и финансируют новые подводные кабели, соединяющие все регионы мира. Правительство США будет продолжать оказывать поддержку американским и другим надежным поставщикам в установке, эксплуатации, техническом обслуживании и ремонте защищенной инфраструктуры, а также продвигать нормативно-правовую среду, которая позволяет продолжать инвестиции.

С 2021 года Государственный департамент США реализует программу CABLES по всему региону Восточной Азии и Тихого океана, ответственно информируя основные заинтересованные стороны телекоммуникационной и кабельной инфраструктуры об опасностях, связанных с выбором ненадежных поставщиков. Соединенные Штаты обеспечили наращивание потенциала для оказания поддержки пяти странам, использующим американские технологии для строительства кабеля Юго-Восточная Азия-Ближний Восток-Западная Европа-6 (SMW6), а также выделили более 22 миллионов долларов США в партнерстве с Австралией и Японией для финансирования строительства кабеля в Восточной Микронезии, строящегося японской фирмой. В октябре 2023 года Соединенные Штаты объявили, что в сотрудничестве с Конгрессом они вместе с Австралией предоставят инвестиции на общую сумму 65 миллионов долларов США для финансирования будущих подводных кабельных соединений для островных стран Тихого океана, чтобы облегчить доступ к мировым рынкам и реализовать региональные цели в области взаимосвязанности. В поддержку этих политических целей Соединенные

Штаты продолжат взаимодействовать с «Большой семеркой» и другими многосторонними группами в целях укрепления надежной, многоуровневой глобальной взаимосвязанности, обеспечивающей разнообразие, устойчивость и избыточность маршрутов данных.

Направление усилий 4: Обеспечение общих интересов в области разработки, использования, отказоустойчивости и безопасности сетей спутниковой связи

Спутниковая связь остается жизненно важным средством соединения мира и обеспечения глобального доступа к информации. Спутники на геостационарной орбите (ГСО) служили этой миссии на протяжении десятилетий и будут продолжать выполнять ее в ближайшие десятилетия. Новые спутниковые технологии, в том числе спутники на низкой околоземной орбите (НОО), приобретают все большее значение для Соединенных Штатов, их союзников и партнеров, поскольку мы работаем над тем, чтобы соединить тех, кто не подключен к Интернету. Распределенный характер распространенных спутниковых группировок обеспечивает отказоустойчивость, и услуги спутниковой связи на низкой околоземной орбите могут все быстрее развертываться для покрытия зон стихийных бедствий или конфликтов. Кроме того, способность спутниковых служб на низкой околоземной орбите обеспечить широкополосной связью практически каждый дюйм планеты повышает вероятность расширения доступа к интернету с соблюдением прав человека, устранения цифрового разрыва и продвижения Целей устойчивого развития ООН.

Американские фирмы лидируют в разработке и развертывании услуг спутниковой связи на ГСО и низкой околоземной орбите, но другие страны, в том числе наши стратегические конкуренты, инвестируют в новые технологические мощности. КНР планирует создать группировку из около 13 000 спутников с четким правительственным мандатом и значительными финансовыми субсидиями. Некоторые государства, обеспокоенные тем, что возможности низкоорбитальных спутников подорвут их способность контролировать информационные потоки, повышают барьеры доступа на рынок, например, устанавливая строгие требования к внутреннему оборудованию или запрещая иностранное владение. Некоторые правительства и неправительственные заинтересованные стороны также выразили обеспокоенность в многосторонних организациях в связи с увеличением количества космического мусора, помех астрономии, увеличением числа случаев радиочастотных помех между низкоорбитальными спутниками или между низкоорбитальными и геостационарными спутниками, а также другими

потенциальными негативными последствиями низкоорбитальных спутниковых сетей. Некоторые страны, хотя и заинтересованы в преимуществах связи, которые могут принести низкоорбитальные спутниковые системы, не знакомы с этими системами и не имеют эффективных режимов для поддержки выхода на рынок и лицензирования. Кроме того, космические системы и активы создают уязвимости в критически важной инфраструктуре США и их союзников, которыми наши противники готовы воспользоваться.

Государственный департамент будет сотрудничать с партнерами и союзниками для достижения общих интересов в разработке, использовании, отказоустойчивости и безопасности низкоорбитальных спутниковых систем. Государственный департамент будет работать над расширением глобального доступа к защищенным услугам через Международный союз электросвязи (МСЭ), устранением барьеров для провайдеров низкоорбитальных спутниковых систем и увеличением многосторонней помощи спутниковым службам в районах с недостаточным уровнем обслуживания. Государственный департамент наряду с другими агентствами также будет содействовать международному сотрудничеству в области исследований и разработок в области низкоорбитальных спутников. Соединенные Штаты также будут продвигать нормы, руководящие принципы и передовой опыт, включая разработку режимов лицензирования и регулирования, для безопасного, безопасного и устойчивого использования низкоорбитальных спутников, а также работать с союзниками и партнерами над повышением кибербезопасности в космосе и устойчивости и безопасности критически важной инфраструктуры.

Направление усилий 5: Повышение эффективности, транспарентности и подотчетности Международного союза электросвязи

Ответственное, дальновидное, инклюзивное и транспарентное лидерство МСЭ в области стандартов электросвязи, развития электросвязи и ИКТ, устранения цифрового разрыва и использования радиочастотного спектра имеет жизненно важное значение для приоритетов США в области развития, обороны и экономики. Соединенные Штаты Америки уже давно поддерживают работу МСЭ в его основных областях компетенции, включая глобальную гармонизацию радиочастотного спектра и содействие развитию мировых сетей электросвязи путем расширения возможности установления соединений и функциональной совместимости. С момента избрания Генерального секретаря Дорин Богдан-Мартин в 2022 году Соединенные Штаты работают с другими государствами-членами и партнерами, чтобы помочь ей реализовать свое видение по расширению цифровой связи и

инклюзивности; укрепление партнерских отношений и сотрудничества с заинтересованными сторонами; расширение прав и возможностей молодежи и вовлечение ее; и повысить организационную эффективность, транспарентность и подотчетность МСЭ для достижения его общих целей.

НАПРАВЛЕНИЕ ДЕЯТЕЛЬНОСТИ 2: Согласование с международными партнерами подходов к цифровому управлению и управлению данными, основанных на соблюдении прав человека

Цифровая солидарность признает необходимость внутреннего управления цифровыми и новыми технологиями, но направлена на разработку общих механизмов, которые помогут поддерживать открытый, функционально совместимый, безопасный и надежный интернет, а также надежные трансграничные потоки данных. Она работает над продвижением политики, основанной на демократических ценностях и уважающей права человека.

Для эффективного продвижения СНБ и НКС продвижение, создание и поддержание безопасной цифровой экосистемы должно сопровождаться усилиями по обеспечению совместимости цифровых технологий и управления данными между союзниками и партнерами путем большей согласованности, взаимного признания и взаимности политики. Государственный департамент наряду с другими федеральными агентствами создает и укрепляет цифровую солидарность путем поддержки надежного потока данных; информационно-разъяснительная работа в поддержку подходов к цифровому управлению и управлению данными с участием многих заинтересованных сторон, основанных на оценке рисков; а также поощрение общих ценностей и принципов управления критически важными и новыми технологиями. Государственный департамент в сотрудничестве с Министерством торговли и другими ведомствами расширяет свои возможности по участию в международных организациях по разработке стандартов и координации с промышленностью и гражданским обществом для обеспечения активного участия заинтересованных сторон США в процессах разработки стандартов и других международных форумах. Соединенные Штаты также работают с союзниками и партнерами над продвижением общего, уважающего права человека видения цифрового будущего; вести переговоры по договору о киберпреступности, уважающему права человека; и защищать целостность информации.

Направление усилий 1: Поддержка надежного потока данных и пропаганда подходов к цифровому управлению и управлению данными с участием многих заинтересованных сторон, основанных на оценке рисков

Цифровая солидарность строится и укрепляется благодаря совместной разработке, гармонизации и взаимному признанию правозащитных подходов к управлению данными и цифровой торговле. В настоящее время эта работа ведется в рамках таких механизмов, как Индо-Тихоокеанская экономическая рамочная программа процветания (IPEF), инициатива «Цифровая трансформация с Африкой» (DTA), Американское партнерство в интересах экономического процветания (APEP), G7, ОЭСР, TTC и Quad.

Соединенные Штаты поддерживают надежный свободный поток данных и открытый Интернет с надежной и эффективной защитой прав человека и неприкосновенности частной жизни, а также мерами по сохранению способности правительств обеспечивать соблюдение законов и продвигать политику в общественных интересах. Законные опасения по поводу конфиденциальности данных могут быть решены с помощью защитных механизмов, которые отслеживают данные, в то же время облегчая трансграничные потоки данных и укрепляя глобальное сотрудничество между правоохранительными органами. Соединенные Штаты будут продолжать отстаивать надежные трансграничные потоки данных, продвигая механизмы передачи данных, которые улучшают взаимодействие между различными режимами конфиденциальности данных. Работая вместе с нашими межведомственными партнерами, Государственный департамент поддержал переговоры и внедрение Рамочной программы конфиденциальности данных между ЕС и США; разработка Декларации ОЭСР о надежном доступе правительства к данным, находящимся в распоряжении частного сектора, в которой определены общие черты в гарантиях конфиденциальности, применяемых демократическими правительствами при доступе к данным в законных целях обеспечения правопорядка и национальной безопасности; а также инициативы по свободному потоку данных с доверием как в G7, так и в ОЭСР. Государственный департамент США сотрудничает с Министерством юстиции США в целях разъяснения применения Закона США «О разъяснении законного использования данных за рубежом» (CLOUD) и ведения переговоров по заключению двусторонних соглашений в соответствии с этим законом.

Наряду с Австралией, Канадой, Японией, Республикой Корея, Мексикой, Филиппинами, Сингапуром и Тайванем в апреле 2022 года Соединенные Штаты запустили Форум по глобальным правилам трансграничной конфиденциальности (CBPR), опираясь на ранее созданную систему CBPR

Азиатско-Тихоокеанского экономического сотрудничества (АТЭС). CBPR предоставляет сертификацию конфиденциальности данных, поддерживаемую соответствующими органами, которая облегчает потоки данных, продвигая совместимые, обязательные к исполнению стандарты защиты данных. Должностные лица из Государственного департамента и Министерства торговли продолжат усилия по привлечению новых стран к соглашению, опираясь на такие усилия, как семинары, проведенные в Кении, Мексике, Чили, Бразилии, Великобритании, Израиле, Иордании, Панаме, Колумбии, Фиджи и Барбадосе, а также в странах АСЕАН.

Несмотря на то, что Соединенные Штаты и их торговые партнеры-единомышленники разделяют во многом одни и те же ценности, у нас часто разные подходы к регулированию цифровой экономики. Правительство США выступает за многосторонние подходы, основанные на оценке рисков, которые нацелены на решение проблем, с которыми мы сталкиваемся, обеспечивая при этом гибкость для реализации преимуществ новых и развивающихся технологий. Односторонние подходы к цифровому налогообложению и взиманию платы за пользование сетью часто не решают основных вопросов доступности и справедливости, заявленных их сторонниками. Кроме того, растущий нарратив о цифровом суверенитете, который был принят некоторыми из наших близких партнеров и союзников, может подорвать ключевые цели цифровой экономики и кибербезопасности. Государственный департамент в сотрудничестве с другими ведомствами будет продолжать выступать против локализации данных, платы за использование сетей, налогов на цифровые услуги, а также других барьеров доступа на рынок, которые способствуют восприятию усиления контроля, но в действительности часто могут подорвать цели роста и безопасности.

Направление усилий 2: Содействие общему пониманию доверия, функционально совместимых стандартов, а также общих ценностей и принципов управления критически важными и новыми технологиями

Одной из наиболее актуальных задач цифровой солидарности является выработка общих подходов к управлению критически важными и новыми технологиями, такими как ИИ. Скорость инноваций, масштаб конкуренции и ставки для наших ценностей, безопасности и процветания требуют согласованных действий. Благодаря технологиям ИИ у нас не будет такой роскоши, как время или преследование узких интересов, которые часто замедляют нашу способность разрабатывать общие принципы и совместимые подходы к регулированию в других частях цифровой экономики.

Формирование общих ценностей и принципов управления в области разработки, развертывания и использования ИИ занимает все более важное место в американской цифровой дипломатии. Соединенные Штаты привлекают союзников, партнеров, частный сектор, гражданское общество, техническое сообщество и другие заинтересованные стороны к обсуждению в рамках «Большой семерки», Глобального партнерства по искусственному интеллекту, Совета Европы, ОЭСР, ООН, ЮНЕСКО и других форумов, чтобы управлять рисками, связанными с ИИ, и обеспечить широкое распространение его преимуществ. Кроме того, нам нужно будет работать вместе, чтобы инвестировать в научные исследования и инфраструктуру, необходимые для измерения, оценки и проверки передовых технологических систем ИИ.

В июле 2023 года президент Байден объявил о добровольных обязательствах семи ведущих компаний в области искусственного интеллекта продвигать безопасную, надежную и прозрачную разработку технологий искусственного интеллекта. Еще восемь компаний (в том числе одна иностранная) подписали эти обязательства в сентябре. Соединенные Штаты интернационализировали и расширили добровольные обязательства в рамках возглавляемого Японией процесса G7 по ИИ в Хиросиме, а в октябре 2023 года лидеры выпустили Международный кодекс поведения для организаций, разрабатывающих передовые системы ИИ. Мы продолжаем работать над расширением признания Кодекса поведения большим количеством стран и компаний за пределами стран-членов G7.

Соединенные Штаты присоединились к двадцати семи другим странам на Саммите по безопасности ИИ в Великобритании и подписали Блетчлийскую декларацию, которая поощряет прозрачность и подотчетность субъектов, разрабатывающих передовые технологии ИИ. Соединенные Штаты и Соединенное Королевство также подписали меморандум о взаимопонимании между соответствующими институтами безопасности ИИ, продвигающий науку измерения, оценки и устранения рисков, связанных с ИИ, в качестве первого шага к глобальному консенсусу по научным основам безопасности ИИ. Эти усилия определяют роль национальных правительств, содействуют международному сотрудничеству и поощряют инновации путем предоставления технически строгих рекомендаций по внедрению безопасной, надежной и заслуживающей доверия технологии ИИ. В то же время USAID и ряд других международных доноров в области развития вступили в партнерство для содействия безопасному, надежному и надежному развитию ИИ в странах с низким и средним уровнем дохода в Африке и других частях мира.

Хиросимские принципы генеративного ИИ

Принимать надлежащие меры на протяжении всей разработки передовых систем ИИ, в том числе до и во время их развертывания и размещения на рынке, для выявления, оценки и снижения рисков на протяжении всего жизненного цикла ИИ.	Разрабатывать и внедрять надежные механизмы проверки подлинности и происхождения контента, где это технически возможно, такие как водяные знаки или другие методы, позволяющие пользователям идентифицировать контент, созданный ИИ.
Выявлять и устранять уязвимости, а также, при необходимости, инциденты и модели неправомерного использования после развертывания, включая размещение на рынке.	Уделять первоочередное внимание исследованиям, направленным на снижение социальных рисков, рисков в области безопасности и безопасности, а также уделять первоочередное внимание инвестициям в эффективные меры по смягчению последствий.
Публично сообщать о возможностях, ограничениях и областях надлежащего и ненадлежащего использования передовых систем ИИ, чтобы обеспечить достаточную транспарентность и тем самым способствовать повышению подотчетности.	Уделять первоочередное внимание разработке передовых систем ИИ для решения самых серьезных мировых проблем, в частности, но не ограничиваясь климатическим кризисом, глобальным здравоохранением и образованием.
Работать над ответственным обменом информацией и отчетностью об инцидентах между организациями, разрабатывающими передовые системы ИИ, в том числе с промышленностью, правительствами, гражданским обществом и научными кругами.	Содействовать разработке и, при необходимости, принятию международных технических стандартов.
Разрабатывать, внедрять и публиковать политики управления ИИ и управления рисками, основанные на риск-ориентированном подходе, включая политики конфиденциальности и меры по смягчению последствий, в частности, для	Внедрять надлежащие меры по вводу данных и защите персональных данных и интеллектуальной собственности.

организаций, разрабатывающих передовые системы ИИ.	
Инвестировать и внедрять надежные средства контроля безопасности, включая физическую безопасность, кибербезопасность и защиту от внутренних угроз на протяжении всего жизненного цикла ИИ.	

В октябре 2023 года президент Байден издал Указ о безопасной, надежной и надежной разработке и использовании искусственного интеллекта. Настоящий Указ устанавливает процесс разработки новых стандартов безопасности и защиты ИИ и направлен на защиту частной жизни граждан, поощрение инноваций и конкуренции, а также продвижение равенства и прав человека. Указ поручил Государственному департаменту укрепить лидерство США за рубежом в вопросах ИИ. Государственный департамент США и Агентство США по международному развитию (USAID) в сотрудничестве с Министерством торговли США возглавляют усилия по созданию Руководства по использованию ИИ в глобальном развитии для использования преимуществ ИИ и управления связанными с ним рисками. В связи с этим Государственный департамент планирует возглавить межведомственную целевую группу по выявлению, проверке подлинности и маркировке синтетического контента, целью которой является содействие обмену информацией, и мобилизация глобальных обязательств как по маркировке аутентичного государственного контента, так и по выявлению синтетического контента. Кроме того, в сотрудничестве с Министерством внутренней безопасности (DHS) Государственный департамент привлекает международных партнеров для оказания помощи в предотвращении, реагировании и восстановлении после потенциальных сбоев в работе критически важной инфраструктуры, вызванных внедрением ИИ в системы критической инфраструктуры или злонамеренным использованием ИИ против этих систем. Государственный департамент и USAID также работают с межведомственными партнерами, включая Национальный институт стандартов и технологий (NIST), Национальный научный фонд (NSF) и Министерство энергетики, над разработкой системы управления рисками в области прав человека в области ИИ и глобальной повестки дня в области исследований в области ИИ.

Кроме того, Государственный департамент США оказывает широкую поддержку Политической декларации об ответственном военном

использовании ИИ и автономии. Несмотря на то, что в Женеве продолжаются важные дискуссии в рамках Конвенции о конкретных видах обычного оружия (КНО), которую Соединенные Штаты будут продолжать поддерживать, сфера этих дискуссий охватывает только одно возможное военное применение ИИ, а именно автономные системы вооружений. Политическая декларация является первой попыткой сформулировать принципы и передовой опыт, охватывающие все сферы применения технологий ИИ в военных целях.

Направление усилий 3: Обеспечение прозрачности, открытости, инклюзивности и беспристрастности процессов по стандартизации

Международные технологические стандарты способствуют развитию технологий, торговле, глобальному экономическому росту и доступу к рынкам, особенно для стартапов и малых и средних предприятий. Они также являются областью стратегической и экономической конкуренции, при этом КНР, в частности, продвигает нисходящие подходы к процессу разработки стандартов и использует свое экономическое влияние для принуждения к поддержке своих предложений по стандартам. В мае 2023 года Белый дом Байдена-Харрис опубликовал первую в истории Стратегию национальных стандартов правительства США для критически важных и новых технологий (USG NSSCET). Как указано в NSSCET правительства США, Соединенные Штаты будут работать с союзниками, партнерами, частным сектором и гражданским обществом для обеспечения того, чтобы разработка международных стандартов охватывала прозрачность, открытость, беспристрастность и консенсус, эффективность и актуальность, согласованность и широкое участие многих заинтересованных сторон. Государственный департамент в сотрудничестве с Министерством торговли и другими ведомствами наращивает потенциал для непосредственного участия в международных организациях по разработке стандартов и координации с промышленностью и гражданским обществом для обеспечения активного участия заинтересованных сторон США в процессах разработки стандартов.

Работая с FCC, NIST, Национальным управлением по телекоммуникациям и информации (NTIA) и другими федеральными агентствами, Государственный департамент поддерживает процессы разработки стандартов для широкого спектра критически важных и новых технологий и платформ, включая IoT, энергетические сети, умные города и подключенные транспортные средства. Соединенные Штаты будут продолжать продвигать и использовать стандарты и руководящие принципы кибербезопасности и конфиденциальности, разработанные NIST, с помощью открытых процессов с тесной связью с международными стандартами.

Этот подход укрепляет политику США в отношении стандартов: подход частного сектора, ориентированный на промышленность с участием правительства, который делает акцент на использовании международных стандартов, разработанных в открытых, прозрачных и основанных на консенсусе процессах. Такая согласованность помогает заинтересованным сторонам снизить бремя международных нормативно-правовых режимов, что приводит к снижению эксплуатационных расходов и лучшему пониманию международной политики. В нем также подчеркивается ценность подхода «снизу-вверх» для других правительств при разработке ими своих приоритетов в области кибербезопасности.

Правительство США разработало формальные и неформальные методы обмена информацией и мониторинга разработки стандартов посредством регулярного взаимодействия с партнерами и союзниками. Например, партнеры Quad и члены TTC подписали меморандумы о сотрудничестве, чтобы обеспечить более широкий обмен информацией, координацию и влияние на разработку международных стандартов. Государственный департамент также поддержал расширение участия в организациях по разработке стандартов из исторически недостаточно представленных стран.

Направление усилий 4: Расширение и диверсификация участия гражданского общества в процессах с участием многих заинтересованных сторон

Соединенные Штаты и их партнеры по-прежнему привержены модели многостороннего управления интернетом и цифровым управлением. Активное и значимое участие всех заинтересованных сторон, включая правительства, гражданское общество, частный сектор, научные круги и техническое сообщество, имеет важнейшее значение для информирования наших дискуссий и разработки политики, содействия прозрачности и подотчетности, а также укрепления реализации и устойчивого развития. В рамках программ помощи иностранным государствам Государственный департамент продвигает политические и информационно-пропагандистские инициативы, в рамках которых заинтересованные стороны гражданского общества взаимодействуют с национальными правительствами, региональными органами управления и международными организациями, устанавливающими стандарты, в целях поощрения политики в области интернета и цифрового управления, соответствующей демократическим ценностям и международным правам человека. Государственный департамент продолжит свои усилия по расширению и диверсификации групп, которые работают над продвижением функционально совместимых, уважающих права человека и безопасных

цифровых технологий. Кроме того, она будет и впредь предотвращать попытки и защищаться от попыток репрессивных правительств исключить гражданское общество и другие заинтересованные стороны из участия в соответствующих форумах.

Соединенные Штаты решительно поддерживают Форум по управлению интернетом (IGF) как выдающийся глобальный орган, объединяющий все заинтересованные стороны в рамках процесса «снизу-вверх» для обсуждения решений вопросов государственной политики в области интернета, основанных на уважении прав человека. Он будет продолжать работать с союзниками и партнерами для поддержания и укрепления значимости IGF.

Направление усилий 5: Продвижение общего, уважающего права человека видения цифрового будущего

Цифровая солидарность основана на общей приверженности управлению технологиями на основе прав человека. Инициатива «Продвижение цифровой демократии» (ADD), запущенная USAID на Саммите за демократию в 2021 году, способствует созданию открытой, безопасной и инклюзивной цифровой экосистемы с помощью таких программ, как партнерство с правительствами, частным сектором и гражданским обществом для укрепления правовой и нормативной базы для данных и цифровых технологий, а также усиление поддержки инженеров-программистов, технологических компаний и исследователей, работающих над внедрением уважения прав человека и демократических ценностей на протяжении всего жизненного цикла технологий. В апреле 2022 года Соединенные Штаты и 60 стран представили Декларацию о будущем интернета (DFI), объединив широкую и разнообразную коалицию партнеров вокруг общего, уважающего права человека видения открытого, функционально совместимого, надежного и безопасного цифрового будущего. В 2023 году, будучи председателем Коалиции за свободу в Интернете, Соединенные Штаты уделяли первоочередное внимание защите основных свобод в Интернете; противодействие неправомерному использованию цифровых технологий и повышение их устойчивости; продвижение норм, принципов и гарантий в области разработки и использования искусственного интеллекта; и расширение охвата цифровыми технологиями. Аналогичным образом, Соединенные Штаты в сотрудничестве с 13 другими странами учредили Глобальное партнерство для действий по борьбе с гендерными домогательствами и злоупотреблениями в Интернете. Это партнерство, возникшее в результате первого Саммита за демократию, является ответом на необходимость решения проблемы гендерного насилия с

использованием технологий в рамках общей глобальной повестки дня по содействию миру, безопасности и стабильности.

Соединенные Штаты продолжат работать с союзниками и партнерами над тем, чтобы цифровые технологии использовались ответственно и с уважением к правам человека. В марте 2023 года Соединенные Штаты вместе с 45 партнерами одобрили Руководящие принципы использования правительствами технологий наблюдения, которые призваны предотвратить неправомерное использование правительствами технологий наблюдения. Кроме того, Государственный департамент продолжит продвигать программы, которые позволяют группам риска, уязвимым и маргинализированным группам населения или тем, кто их защищает, готовиться, предотвращать, выявлять, расследовать и получать средства правовой защиты от цифровых злоупотреблений или других видов цифровых репрессий.

Соединенные Штаты поддерживают ряд многосторонних инициатив, направленных на решение целого ряда проблем в Интернете при соблюдении свободы мнений и их выражения, в том числе Крайстчерчский призыв к действиям в 2019 году, возглавляемую Францией Лабораторию защиты детей в онлайновой среде, Коалицию за свободу в Интернете и Глобальное партнерство для действий по борьбе с гендерными домогательствами и злоупотреблениями в Интернете. Соединенные Штаты будут и впредь выступать за подход, основанный на уважении прав человека, в соответствии с защитой свободы мнений и их выражения и поощрением гендерного равенства и равенства, в то время как правительства по всему миру предлагают ужесточить регулирование онлайн-платформ.

Дальнейшее укрепление внутренней политики позволит углубить координацию с международными партнерами по целому ряду цифровых вопросов. Например, Указ Президента о безопасном, надежном и надежном развитии и использовании искусственного интеллекта укрепил позицию Соединенных Штатов в международных дискуссиях по вопросам управления ИИ. Национальная стратегия кибербезопасности поддерживает законодательные усилия по установлению строгих, четких ограничений на возможность сбора, использования, передачи и хранения персональных данных и обеспечению надежной защиты конфиденциальных данных, таких как геолокация и медицинская информация. NCS специально призывает к тому, чтобы это законодательство смягчило риски конфиденциальности, возникающие при обработке данных, и установило национальные требования к защите персональных данных.

Направление усилий 6: Ведение переговоров по договору о киберпреступности, уважающему права человека

Соединенные Штаты, их союзники и партнеры, а также группы гражданского общества уже давно поддерживают Конвенцию Совета Европы о киберпреступности (широко известную как Будапештская конвенция) как наиболее эффективный инструмент для обеспечения глобальных стандартов криминализации злонамеренной кибердеятельности, получения электронных доказательств и содействия международному сотрудничеству в области компьютерных преступлений. Конвенция была разработана таким образом, чтобы быть глобальной и открытой для всех регионов. Семьдесят две страны, включая Соединенные Штаты, в настоящее время являются участниками Конвенции, и еще 21 стране было предложено присоединиться.

Поддерживая присоединение к Будапештской конвенции, Соединенные Штаты и их партнеры также активно работают над тем, чтобы переговоры в Специальном комитете ООН по разработке конвенции против киберпреступности привели к положительному результату: договору о киберпреступности, уважающему права человека, который позволил бы всем государствам-членам ООН лучше сотрудничать в борьбе с киберпреступностью. Соединенные Штаты и их партнеры будут и впредь выступать против чрезмерно широких определений киберпреступности, которые могут быть использованы для подавления свободы выражения мнений, посягательства на неприкосновенность частной жизни и/или создания опасности для отдельных лиц и сообществ. Соединенные Штаты также будут продолжать выступать за необходимые и достаточные гарантии, соизмеримые с масштабами внутренних полномочий и международного сотрудничества, предусмотренного Конвенцией. Поддержание открытого, инклюзивного и прозрачного процесса наилучшим образом позволит государствам вести переговоры по юридически обязывающему соглашению с участием заинтересованных сторон.

Направление усилий 7: Защита целостности информации

Проблемы целостности информации не новы, но решительные противники иностранных государств и быстрый технологический прогресс, особенно взаимодействие человека и машины на основе ИИ, создают сложную динамику, которая усугубляет информационные риски, обеспечивая быстрое, крупномасштабное и целенаправленное распространение синтетического контента с использованием ИИ. Создание устойчивой информационной среды, в которой ведутся открытые, свободные публичные дебаты и постоянный доступ к разнообразным источникам информации, основанной на фактах,

является неизменным приоритетом для Соединенных Штатов, их союзников и партнеров. Эти особенности необходимы гражданам для формирования своего мнения и осуществления своих прав человека, включая свободу выражения мнений, свободу мирных собраний и ассоциаций, а также право голоса. Манипулирование информацией является дестабилизирующим и может нанести ущерб национальной безопасности, демократическим процессам, экономическому благосостоянию, окружающей среде, реагированию на кризисы, правам человека и общественному здравоохранению. В то время как иностранные субъекты, стремящиеся вмешиваться в информационную среду или манипулировать ею, создают значительные риски, существуют дополнительные проблемы, с которыми сталкиваются открытые общества, связанные с качеством информации в Интернете и подрывом доверия.

Вместе с союзниками и партнерами Государственный департамент продолжит работу по повышению информационной устойчивости гражданского населения, противодействию иностранной государственной и негосударственной экстремистской пропаганде в Интернете и снижению рисков ИИ для целостности информации, защищая при этом свободу выражения мнений. Правительство США будет работать над защитой честности выборов и других демократических процессов во всем мире. В ТТС, ОЭСР и G7 Соединенные Штаты разрабатывают общие подходы к построению здоровых и устойчивых информационных экосистем. Соединенные Штаты и Франция являются сопредседателями Центра информационных ресурсов DIS/MIS, ведущей инициативы ОЭСР по обеспечению целостности информации. В Центре Государственный департамент сосредоточен на расширении сотрудничества в области обмена передовым опытом и укреплении информационной устойчивости как между странами ОЭСР, так и странами, не входящими в ОЭСР, а также на разработке основ для руководства усилиями всего общества в этой области. В рамках Инициативы по содействию целостности и устойчивости информации (Pro-Info) USAID стремится укрепить здоровые информационные экосистемы и помочь бороться с манипулированием информацией путем привлечения многих заинтересованных сторон, координации доноров и усилий по наращиванию потенциала.

На третьем Саммите за демократию в 2024 году Соединенные Штаты представили демократическую дорожную карту по повышению гражданской устойчивости к глобальным цифровым манипуляциям, в которой подчеркивается важность проблемы манипулирования цифровой информацией как угрозы функциональности и жизнеспособности общества; признает, что обеспечение целостности информации может быть совместимо со свободой

мнений и их свободное выражение; укрепляет способность цифровых платформ частного сектора укреплять гражданскую устойчивость; и уделяет первоочередное внимание усилиям по решению проблемы генеративного ИИ (GAI), особенно в контексте глобальных выборов 2024 года. Соединенные Штаты также одобрили Глобальную декларацию о целостности информации в Интернете, принятую Канадой и Нидерландами. Декларация, основанная на международном праве в области прав человека, устанавливает международные обязательства государств-участников на высоком уровне по защите и поощрению целостности информации в Интернете.

Кроме того, Государственный департамент объявил о создании Рамочной программы по противодействию манипулированию информацией иностранных государств. Эта Рамочная программа направлена на выработку общего понимания угрозы и установление общего набора областей действий, в которых Соединенные Штаты вместе со своими союзниками и партнерами могут разработать скоординированные меры реагирования на иностранные информационные манипуляции и защитить свободные и открытые общества.

НАПРАВЛЕНИЕ ДЕЯТЕЛЬНОСТИ 3: Содействие ответственному поведению государств в киберпространстве и противодействие угрозам киберпространству и критически важной инфраструктуре путем создания коалиций и привлечения партнеров

В ООН и региональных органах безопасности Соединенные Штаты вместе со своими союзниками и партнерами работают над продвижением ответственного поведения государств в киберпространстве на основе одобренных Генеральной Ассамблеей ООН рамок, подкрепленных применимостью существующего международного права, соблюдением общепризнанных и добровольных норм поведения государств в мирное время, разработкой и реализацией мер доверия для снижения риска конфликтов в киберпространстве. а также приверженность наращиванию потенциала государств для реализации элементов рамочной программы.

Несмотря на глобальный консенсус в отношении рамок ответственного поведения в киберпространстве, эти нормы не являются самообеспечивающимися. Некоторые государства действуют вопреки ей. Когда государство участвует в значительной деструктивной, подрывной или иным образом дестабилизирующей злонамеренной кибердеятельности, противоречащей рамкам, ответственные государства должны сотрудничать, чтобы привлечь это безответственное государство к ответственности.

Цифровая солидарность в этом контексте демонстрируется постоянной взаимной поддержкой и скоординированными кампаниями. Соединенные Штаты и их партнеры обмениваются информацией о киберугрозах, чтобы помочь повысить устойчивость к вредоносным действиям и пресечь их; проявлять солидарность с жертвами, помогая реагировать на серьезные инциденты, тем самым сигнализируя противникам, что они не могут изолировать страну-мишень с помощью злонамеренных операций; и обеспечить подотчетность за деструктивную, подрывную и иным образом дестабилизирующую кибердеятельность совместно со странами-единомышленниками. Соединенные Штаты и некоторые союзники также подтвердили применение в киберпространстве своих обязательств по договорам о взаимной обороне. Кроме того, Государственный департамент и другие федеральные агентства работают с союзниками и партнерами над пресечением деятельности программ-вымогателей и других преступных сетей и защитой демократических процессов и институтов. Заглядывая в будущее, Соединенные Штаты продолжат подобные усилия по продвижению ответственного поведения в киберпространстве и противодействию угрозам киберпространству и нашей критически важной инфраструктуре путем создания коалиций и привлечения партнеров.

Направление усилий 1: Продолжение практических дискуссий, ориентированных на имплементацию норм в ООН

В результате последовательного взаимодействия на протяжении почти двух с половиной десятилетий и четырех предыдущих администраций была выработана система ответственного поведения государств в киберпространстве, неоднократно поддерживаемая всеми членами Генеральной Ассамблеи ООН, которая подтверждает применимость международного права к использованию государствами информационно-коммуникационных технологий, подтверждает приверженность добровольным нормам ответственного поведения государств в мирное время. и предлагает практические меры по укреплению доверия, способствующие снижению риска конфликтов, связанных с киберинцидентами. Эта концепция лежит в основе нашего видения киберпространства, в котором государства ведут себя надлежащим образом, управляют риском нежелательной эскалации, привлекают злоумышленников к ответственности за безответственные действия и работают вместе для реагирования на серьезные киберинциденты и восстановления после них. Однако выполнение этих норм имеет решающее значение для их эффективности.

Мы продолжим более целенаправленные дискуссии в ООН, посвященные тому, как государства-члены и институты могут работать вместе для реализации основных элементов Рамочной программы и наращивания потенциала всех государств по борьбе с киберугрозами. Чтобы приспособиться к этому развивающемуся диалогу, Соединенные Штаты и их партнеры предложили создать в ООН более ориентированный на действия форум – Программу действий (ПДД) – в качестве будущего постоянного механизма для диалога по кибервопросам, связанным с международной безопасностью. Разработанная таким образом, чтобы быть достаточно гибкой для противодействия будущим угрозам, с государствами-членами, определяющими ее направление с течением времени, POA также будет включать в себя мнения гражданского общества, частного сектора и других негосударственных заинтересованных сторон.

В рамках продвижения ответственного поведения государств в киберпространстве Соединенные Штаты и наши партнеры также продолжат совместную работу в рамках региональных форумов по безопасности и других форумов, таких как Организация по безопасности и сотрудничеству, Организация американских государств и Региональный форум АСЕАН, по разработке и реализации мер по укреплению кибердоверия.

Направление усилий 2: Нарушение и повышение устойчивости к вредоносным действиям состояния

Учитывая взаимосвязанный характер киберпространства, международное сотрудничество имеет решающее значение для пресечения, срыва и противодействия действиям противника в киберпространстве и через него.

Государственный департамент возглавляет усилия, в том числе по содействию международной информационно-разъяснительной работе, по противодействию растущей угрозе подрывных или разрушительных кибератак на критически важную инфраструктуру Соединенных Штатов, их союзников и партнеров. Это включает в себя обмен по дипломатическим каналам совместными рекомендациями по кибербезопасности с Агентством по кибербезопасности и безопасности инфраструктуры (CISA), Федеральным бюро расследований (ФБР) и Агентством национальной безопасности (АНБ), а также с союзниками и партнерами по угрозам; наращивание потенциала и обмен информацией с новыми и существующими партнерами для смягчения киберугроз и обеспечения устойчивости их критически важной инфраструктуры; а также использование двусторонних, многосторонних и других форумов для разъяснения и информирования ожиданий в отношении

соблюдения международного права и рамок ответственного поведения в киберпространстве. Кроме того, члены Quad разработали совместные принципы кибербезопасности критически важной инфраструктуры, а члены НАТО взяли на себя обязательство обеспечивать устойчивость критически важной инфраструктуры, усиленную защиту критически важной инфраструктуры посредством обучения и учений, а также обмениваться разведданными об угрозах.

В рамках своей деятельности по борьбе с противником в киберпространстве Государственный департамент обеспечивает руководство внешней политикой и использует дипломатические обязательства для поддержки усилий Министерства обороны (МО) по проведению кампаний в киберпространстве и через него ниже уровня вооруженного конфликта для усиления сдерживания и срыва противников. Как указано в Киберстратегии Министерства обороны США на 2023 год, Киберкомандование США продолжает обороняться, чтобы обнаруживать, разоблачать и защищаться от источников злонамеренной кибердеятельности, а также укреплять ответственное поведение государств путем поощрения соблюдения международного права и международно признанных норм киберпространства. В Киберстратегии МО США также отмечается, что кибероперации наиболее эффективны, когда они используются в сочетании с другими инструментами национальной мощи, включая дипломатическое взаимодействие и наращивание киберпотенциала.

Государственный департамент в тесной координации с межведомственными и международными партнерами будет продолжать организовывать и проводить постоянные кампании дипломатического давления с целью повышения осведомленности международного и общественного сообщества о значительных киберугрозах и увеличения затрат и рисков для злоумышленников. Например, Соединенные Штаты работали с союзниками, партнерами и частным сектором, чтобы сорвать усилия КНДР по получению доходов с помощью киберпреступности, кражи криптовалют и ИТ-работников. Киберкомандование США, АНБ, МВБ, Минюст и ФБР разоблачили северокорейское вредоносное ПО, конфисковали вредоносную киберинфраструктуру, конфисковали криптовалюту и фиатную валюту, а также поделились с частным сектором оперативной информацией об угрозах. Государственный департамент координирует действия с Республикой Корея через двустороннюю Рабочую группу по кибербезопасности КНДР, включая обмен информацией и координацию политики. Кроме того, США, Япония и Республика Корея координируют усилия по противодействию киберугрозам КНДР в рамках трехсторонней рабочей группы, о создании которой было

объявлено в ходе саммита в Кэмп-Дэвиде в августе 2023 года. Государственный департамент также проинформировал официальных лиц по всему миру об угрозах, исходящих от ИТ-работников и киберпреступников КНДР, и выделил средства иностранной помощи для наращивания потенциала для обнаружения и защиты от кибер- и криптоугроз КНДР.

Направление усилий 3: Поддержка союзников и партнеров в условиях злонамеренной деятельности

Ключевым элементом цифровой солидарности является поддержка партнеров, когда они сталкиваются с серьезными разрушительными или дестабилизирующими киберинцидентами. Государственный департамент продолжит работать с союзниками и партнерами – через наши посольства на местах и наших экспертов по кибербезопасности в Вашингтоне – для координации надлежащей поддержки во время расследования, смягчения последствий и восстановления после таких киберинцидентов. Эта поддержка может включать, в зависимости от обстоятельств, предоставление консультаций экспертами посольства по кибербезопасности; содействие проведению удаленных или оперативных расследований, охоты и анализа вредоносных программ; проекты иностранной помощи; или координация усилий по оказанию помощи в киберпространстве со странами-партнерами. Государственный департамент рассматривает такую деятельность как важнейшую для укрепления коллективной киберзащиты и устойчивости, а также для оказания помощи странам в противостоянии кибератакам, направленным на принуждение или иное вмешательство в их суверенитет.

Направление усилий 4: Привлечение к ответственности безответственных государств

Для эффективного сдерживания наших противников и противодействия злонамеренным действиям ниже порога вооруженного конфликта мы будем продолжать работать с нашими союзниками и партнерами, чтобы осудить эту деятельность и наложить значимые последствия. В этих усилиях используются все инструменты государственного управления, включая дипломатическую изоляцию, правоохранительные органы, контркибероперации и экономические санкции. В сентябре 2019 года 27 стран публично пообещали в Совместном заявлении под руководством США о содействии ответственному поведению государств в киберпространстве добровольно сотрудничать в целях привлечения государств к ответственности, когда они действуют вопреки Рамочным правилам. Число государств, готовых публично призвать государства к ответственности, достигло 39 в июле 2021 года, когда НАТО, ЕС,

Австралия, Канада, Новая Зеландия, Великобритания и Япония публично осудили причастность КНР к инциденту с утечкой данных на сервере Microsoft Exchange и другим злонамеренным кибердействиям. Совсем недавно коалиции единомышленников связывали кибератаку России на спутниковую сеть связи KA-SAT компании Viasat накануне ее вторжения в Украину и выражали солидарность с Албанией в связи с разрушительными кибероперациями Ирана. Соединенные Штаты продолжат работать над расширением коалиции тех, кто готов привлечь государства к ответственности за подрывную и дестабилизирующую киберактивность, и использовать соответствующие многосторонние группировки для взаимной поддержки и оказания помощи жертвам такого поведения.

Направление усилий 5: Подтвердить применение договоров о взаимной обороне с некоторыми союзниками в киберпространстве

В соответствии с давним признанием США того, что в киберпространстве применимо существующее международное право, в киберпространстве могут применяться обязательства по договорам и другим международным соглашениям. За последние несколько лет Соединенные Штаты и некоторые союзники выступили с публичными заявлениями, подтверждающими применение в киберпространстве обязательств по их соответствующим договорам о взаимной обороне, включая Договор о безопасности 1951 года между Австралией, Новой Зеландией и Соединенными Штатами (АНЗЮС) (2011 год); Североатлантический договор (2014 г.); Договор о взаимном сотрудничестве и безопасности между США и Японией (2019 г.); и Договор о взаимной обороне между Соединенными Штатами Америки и Республикой Корея (2023 г.). Государственный департамент и Министерство обороны продолжат совместную работу с союзниками по НАТО для участия в предварительном планировании действий в чрезвычайных ситуациях и дальнейшего повышения осведомленности партнеров по альянсу о том, что существующие договоры о взаимной обороне могут применяться в киберпространстве и что кибератаки, достигающие уровня вооруженного нападения, могут повлечь за собой обязательства по взаимной обороне в соответствии с такими договорами.

Направление усилий 6: Противодействие преступникам и программам-вымогателям

Для многих стран самым большим риском для их цифровой безопасности и экономики является онлайн-мошенничество, преступный взлом и другие финансовые преступления. В частности, в последние годы

программы-вымогатели стали явной угрозой национальной безопасности, общественной безопасности и экономическому процветанию. Действуя из безопасных гаваней, таких как КНР, КНДР, Иран, Россия и некоторые другие страны, операторы программ-вымогателей нарушают работу государственных служб, больниц, школ, трубопроводов и организаций гражданского общества. В связи с тем, что некоторые государства используют злоумышленников-вымогателей в качестве посредников или закрывают глаза на их деятельность и значительное влияние их кибератак на критически важную инфраструктуру, становится все более очевидным, что деятельность программ-вымогателей может угрожать международному миру и безопасности. Цифровая солидарность четко выражается в усилиях Государственного департамента по использованию своих дипломатических возможностей для поддержки общегосударственной борьбы с программами-вымогателями и другими формами киберпреступности, в том числе путем наращивания потенциала партнеров; создание коалиций для предотвращения, пресечения и наказания преступного поведения; и содействие сотрудничеству с частным сектором.

Государственный департамент, Министерство внутренней безопасности и Министерство юстиции продолжат участвовать в работе Объединенной целевой группы США по борьбе с программами-вымогателями и сотрудничать с частным бизнесом и международными союзниками для разрушения преступной инфраструктуры и ресурсов в Интернете, уничтожения ботнетов и конфискации криптовалюты, полученной в результате кампаний программ-вымогателей. Например, программа США «Глобальная сеть правоохранительных органов по борьбе с транснациональными преступлениями и преступлениями в сфере высоких технологий» (GLEN) — давнее партнерство между Государственным департаментом и Министерством юстиции — представляет собой глобальную сеть по наращиванию потенциала правоохранительных органов, состоящую из региональных консультантов Министерства юстиции США по международному компьютерному взлому и интеллектуальной собственности (ICHIP), компьютерных криминалистов и федеральных правоохранительных органов. Двенадцать адвокатов-консультантов ICHIP работают по всему миру. Советник ICHIP, базирующийся в Гааге, способствовал сотрудничеству между Соединенными Штатами, Францией, Германией, Нидерландами, Великобританией, Румынией и Латвией в крупнейшей в истории ликвидации ботнета и вредоносного ПО, известного как Qakbot, в августе 2023 года. Сеть также проводит обучение и оказывает техническую помощь иностранным партнерам в правоохранительных органах, прокуратуре и судебным органам в борьбе с кражей интеллектуальной собственности и киберпреступностью, а также в оказании помощи в сборе и

использовании электронных доказательств для борьбы со всеми видами преступлений. Программа повышает безопасность США, сокращая использование иностранной вычислительной инфраструктуры для вредоносных действий, нацеленных на сети США, и демонстрируя, что ни один злоумышленник не может уклониться от верховенства закона.

GLEN создал пять региональных рабочих групп по криптовалютам по всему миру, которые занимаются обменом информацией и наращиванием потенциала для борьбы с преступным неправомерным использованием криптовалюты, в том числе в программах-вымогателях. Дополнительные приоритеты в области наращивания потенциала включают борьбу с интернет-мошенничеством и борьбу с растущим бедствием сексуальной эксплуатации детей и сексуальных надругательств над детьми в Интернете.

Государственный департамент продолжит использовать свои дипломатические усилия и наращивание потенциала для расширения и укрепления участия в Международной инициативе по борьбе с программами-вымогателями (CRI). CRI — это уникальная и географически разнообразная коалиция, в которую входят почти 60 стран, а также многосторонние институты, такие как Европейский союз, Интерпол и Организация американских государств, которые стремятся повысить коллективную устойчивость к программам-вымогателям, сотрудничать в борьбе с программами-вымогателями и преследовать виновных, противодействовать незаконному финансированию, лежащему в основе экосистемы программ-вымогателей, и работать с частным сектором для защиты от атак программ-вымогателей. В дополнение к CRI Государственный департамент в координации с Объединенной целевой группой США по борьбе с программами-вымогателями продолжит развивать двусторонние и многосторонние усилия, направленные на то, чтобы отбить у государств охоту спонсировать программы-вымогатели или позволять киберпреступникам использовать свою территорию в качестве убежища.

Работа CRI поддерживает реализацию рамок ответственного поведения государств в киберпространстве, включая добровольную норму о том, что «государства должны отвечать на соответствующие просьбы об оказании помощи со стороны другого государства, чья критически важная инфраструктура подвержена злонамеренным действиям в области ИКТ», в дополнение к «соответствующим запросам о смягчении злонамеренной деятельности в области ИКТ, направленной на критически важную инфраструктуру другого государства, исходящей с их территории, с учетом уважения суверенитета».

Направление усилий 7: Защита демократических процессов и институтов

Учитывая, что в 2024 году выборы пройдут более чем в 70 странах и почти половине населения мира, их уязвимость к кибервмешательству, включая потенциальные кибератаки, которые могут нарушить избирательные процессы; шпионаж, слежка и запугивание политиков, активистов и журналистов; Особенно остро стоит злонамеренная деятельность по оказанию влияния с использованием кибертехнологий, направленная на то, чтобы повлиять на результаты выборов и подорвать доверие общественности к выборам. Соединенные Штаты публично и на международных мероприятиях подчеркивали, что считают избирательную инфраструктуру частью критически важной инфраструктуры. Он также отметил усилия некоторых государств по использованию киберсредств для дестабилизации демократических процессов. Соединенные Штаты, их союзники и партнеры будут продолжать разоблачать и защищаться от злонамеренных операций, направленных на дестабилизацию демократических процессов и общества, в том числе путем обмена информацией об угрозах и укрепления устойчивости избирательных комиссий и других ключевых институтов. Например, в 2023 году Соединенные Штаты присоединились к усилиям Соединенного Королевства по привлечению поддерживаемых Россией злоумышленников и хакеров к операциям, нацеленным на британских политиков и демократические процессы. Эти дипломатические усилия сопровождались тем, что Министерство юстиции одновременно объявило об уголовных обвинениях против двух ответственных лиц.

Направление усилий 8: Борьба с распространением и неправомерным использованием коммерческих шпионских программ

Распространение и неправомерное использование коммерческого шпионского ПО представляет собой серьезную угрозу как для национальной безопасности США, включая интересы контрразведки, так и для демократических ценностей и прав человека во всем мире, позволяя осуществлять слежку, репрессии и преследования журналистов, правозащитников, антикоррупционных активистов и других членов гражданского общества. В марте 2023 года президент Байден подписал указ, ограничивающий оперативное использование правительством США коммерческого шпионского ПО, которое представляет значительные риски для контрразведывательной деятельности или безопасности Соединенных Штатов или значительные риски ненадлежащего использования, включая нарушение прав человека, иностранным правительством или иностранным лицом. В то же

время Государственный департамент выпустил Совместное заявление об усилиях по противодействию распространению и неправомерному использованию коммерческих шпионских программ с 10 другими странами, обязавшимися предпринять конкретные усилия по противодействию неправомерному использованию и распространению коммерческого шпионского ПО, к которому еще 6 стран присоединились в марте 2024 года.

В дальнейшем правительство США будет продолжать работать над тем, чтобы препятствовать неправомерному использованию и позитивно изменить рынок коммерческого шпионского ПО, вытесняя или поощряя реформы со стороны предприятий, связанных с неправомерным использованием этих инструментов. Государственный департамент продолжит дипломатическое взаимодействие, чтобы призвать страны, которые уже присоединились к Совместному заявлению, предпринять конкретные шаги по противодействию неправомерному использованию и распространению коммерческого шпионского ПО, побудить другие страны присоединиться к нему и убедить страны, которые неправильно используют или допускают неправомерное использование шпионского ПО, принять меры предосторожности, чтобы меньше отклоняться от политики США. Государственный департамент продолжит сотрудничать с Министерством торговли и Министерством финансов США, чтобы обеспечить привлечение к ответственности тех, кто злоупотребляет коммерческими шпионскими программами с помощью таких инструментов, как санкции, визовые ограничения и экспортный контроль. Кроме того, Государственный департамент продолжит поднимать этот вопрос на многосторонних и общественных форумах, а также тесно взаимодействовать с гражданским обществом, журналистами, технологическими платформами и инвестиционным сообществом.

НАПРАВЛЕНИЕ ДЕЯТЕЛЬНОСТИ 4: Укрепление и наращивание международной партнерской политики в области цифровых технологий и киберпотенциала

Мероприятия по наращиванию потенциала в области цифровых технологий и кибербезопасности являются мощными признаками цифровой солидарности в действии. Они помогают партнерам создавать безопасную, разнообразную и устойчивую инфраструктуру ИКТ и развивать глобальные рынки функционально совместимых и безопасных товаров и услуг ИКТ. Они также имеют решающее значение для стран с формирующимся рынком для достижения ЦУР.

Противники, и в частности КНР, понимают это и стремятся превзойти Соединенные Штаты и партнеров-единомышленников, предлагая комплексную поддержку развития ИКТ, начиная с комплексных программ обучения и заканчивая высшим образованием и стипендиями. Государственный департамент в сотрудничестве с другими федеральными агентствами, международными союзниками и партнерами, а также частным сектором стремится мобилизовать технологии, процессы и людей для поддержки экономических целей и целей развития наших партнеров. Эта помощь часто оказывает каталитическое воздействие, побуждая страны-партнеры уделять первоочередное внимание кибербезопасности и повышению устойчивости к внешним воздействиям. Это также способствует лучшему пониманию преимуществ подходов к кибербезопасности и цифровой политике, за которые выступают Соединенные Штаты.

Стремясь усилить цифровую солидарность в сфере иностранной помощи, USAID запустило Донорские принципы прав человека в цифровую эпоху в партнерстве с Исследовательским центром международного развития Канады (IDRC) и в сотрудничестве с Государственным департаментом. Эти принципы, одобренные правительствами 38 стран-партнеров, предлагают единую основу и набор критериев для продвижения инклюзивного, уважающего права человека подхода к иностранной помощи по вопросам цифровых технологий.

Для достижения поставленных целей мы должны работать над тем, чтобы мы могли действовать быстро и эффективно, удовлетворяя потребности иностранных партнеров в реагировании на инциденты, надежном развитии инфраструктуры и наращивании потенциала.

Направление усилий 1: Поддержка и расширение усилий по наращиванию потенциала в области цифровой политики, законодательства и регулирования

Для того чтобы цифровая инфраструктура могла эффективно служить населению, странам необходимо иметь соответствующую нормативно-правовую базу. Недостаточно продвигать безопасную, устойчивую технологическую инфраструктуру; Для обеспечения значимой взаимосвязанности должна существовать эффективная, прозрачная, гибкая и технологически нейтральная нормативно-правовая база. Таким образом, иностранная помощь США сосредоточена на разработке и укреплении соответствующей законодательной и нормативной базы, а также на наращивании местного технического потенциала и решении кадровых вопросов.

Государственный департамент продолжит предоставлять партнерам экспертные знания и профессиональную подготовку, необходимые им для разработки и управления безопасными, уважающими права человека цифровыми экосистемами. Благодаря технической помощи, наращиванию потенциала в области политики в области ИКТ и электросвязи, а также грантам на обучение, DCCP способствовал проведению законодательных и регуляторных реформ, способствующих конкуренции. Например, проект «Продвижение американских подходов к политике и регулированию в области ИКТ» (ProICT), еще один проект DCCP, возглавляемый Государственным департаментом и USAID, помог расчистить путь для новых участников рынков 5G и обеспечил техническую консультативную поддержку аукциона по продаже спектра 5G.

Государственный департамент, USAID, NTIA и FCC, работая с промышленностью и частным сектором, продолжат предоставлять учебные программы и техническую помощь должностным лицам развивающихся стран, участвующим в управлении спектром, развертывании беспроводных и спутниковых технологий и приобретении облачных услуг.

Направление усилий 2: Расширение усилий партнеров по наращиванию потенциала в области кибербезопасности

Усилия по наращиванию киберпотенциала, которые обычно сосредоточены на укреплении способности страны принимать и разрабатывать киберполитику и стратегии или улучшать ее технические возможности по обнаружению, реагированию и восстановлению после киберинцидентов, оказывают прямое и положительное влияние на международную киберстабильность и безопасность граждан США. Помощь, направленная на разработку политики и стратегии, повышает доверие к государствам и их участие в международных дискуссиях. Она предоставляет им возможности на национальном уровне, необходимые для реализации норм, разработанных в рамках рамок ответственного поведения государств в киберпространстве, для соблюдения стандартов Будапештской конвенции о киберпреступности, для привлечения к ответственности безответственных субъектов в киберпространстве и для разработки подхода на национальном уровне к противодействию постоянным киберугрозам и повышению долгосрочной устойчивости. Улучшение оперативных возможностей партнеров повышает вероятность того, что они смогут бороться с транснациональными угрозами киберпреступности, обмениваться полезной информацией о киберугрозах и инцидентах с Соединенными Штатами, а также успешно сотрудничать с

Соединенными Штатами в операциях по пресечению злонамеренной киберактивности.

В течение последних двух десятилетий Государственный департамент сотрудничал с другими агентствами, международными партнерами, региональными организациями и частным сектором в целях наращивания киберпотенциала за рубежом. Официальные лица и специалисты частного сектора со всего мира принимают участие в семинарах по промышленным системам управления, проводимых совместно с CISA. Соединенные Штаты оказывают содействие усилиям Организации американских государств в таких областях, как реагирование на киберинциденты, разработка и реализация национальной стратегии кибербезопасности, осведомленность в области кибербезопасности и подготовка киберкадровых ресурсов. Соединенные Штаты являются ведущим донором программ Совета Европы, направленных на расширение принятия Будапештской конвенции о киберпреступности. Глобальный форум по экспертизе в области кибербезопасности (GFCE), одним из основателей и активным членом которого являются Соединенные Штаты, предоставляет глобальную платформу для установления связей между политиками, практиками и экспертами в области кибербезопасности, а также для согласования программ помощи с получателями.

Многие агентства оказали поддержку международным партнерам в использовании и адаптации Концепции кибербезопасности NIST, а Государственный департамент поддержал международное участие в разработке версии 2.0 этой структуры. Программа NICE Workforce Framework for Cybersecurity (NICE Framework) была использована для поддержки развития и управления талантами. Министерство торговли, NIST, USAID и Государственный департамент будут привлекать международных партнеров для содействия разработке критически важных и новых технологических стандартов в таких областях, как передовой опыт в отношении сбора, обработки, конфиденциальности, обработки и анализа данных; надежность, верификация и гарантия систем ИИ и управление рисками ИИ; а также аутентификация и происхождение контента, обнаружение синтетического контента и маркировка контента. Кроме того, NIST выбрал четыре алгоритма, предназначенных для противостояния кибератакам квантовых компьютеров, и разрабатывает стандарты для использования правительством США. Государственный департамент США будет работать с NIST над интернационализацией, в том числе посредством постоянного взаимодействия с международными органами по стандартизации, этих постквантовых стандартов криптографии, чтобы организации по всему миру могли интегрировать их в свою инфраструктуру шифрования. Они также продолжат

привлекать международных партнеров к разработке и внедрению лучших практик кибербезопасности в таких областях, как модель "Никому не доверяй", кибербезопасность IoT, цифровая идентификация, операционные технологии, безопасность программного обеспечения и управление рисками в цепочке поставок.

Государственный департамент продолжит тесную координацию с Министерством обороны, Министерством юстиции, Министерством внутренней безопасности, CISA, NIST, NTIA, USAID, Министерством финансов США, Министерством энергетики, Министерством торговли и другими федеральными агентствами, чтобы обеспечить поддержку стратегических интересов и поддержку многочисленных потоков наращивания потенциала.

Направление усилий 3: Разработка новых инструментов для быстрого и эффективного оказания цифровой и киберпомощи

Спрос на помощь в области кибербезопасности и киберпреступности, в частности на киберзащиту, реагирование на инциденты и навыки борьбы с преступным неправомерным использованием криптовалюты, растет в масштабах. После кибератак на Украину, Коста-Рику и Албанию Соединенные Штаты и их союзники обменивались разведданными об угрозах; содействие оперативному сотрудничеству; обеспечили доступ к сервисам коммерческих компаний, занимающихся кибербезопасностью, включая аппаратное и программное обеспечение, а также встроенную техническую поддержку; и финансировал долгосрочное наращивание потенциала.

Из этих и других случаев Государственный департамент понял важность регулярной и тесной координации между правительством США и международными партнерами, а также важность мобилизации технологий и опыта частного сектора. Модернизация органов и механизмов для предоставления иностранной помощи в области технологий с необходимой скоростью и в необходимых масштабах имеет решающее значение. Мы должны адаптировать наши ресурсы и органы внешней помощи для поддержки долгосрочного лидерства США и укрепления цифровой солидарности.

Признавая настоятельную и растущую потребность в дополнительных инструментах для продвижения внешней политики США в киберпространстве и цифровом пространстве, Конгресс создал в соответствии с Законом об ассигнованиях Государственного департамента от 2023 года и профинансировал через Закон об ассигнованиях на зарубежные операции и связанные с ними программы Государственного департамента 2024 года Фонд киберпространства, цифровой связи и связанных с ними технологий. Этот

фонд предоставит Государственному департаменту полномочия и целевое финансирование для поддержки стратегически важных программ помощи иностранным государствам, связанным с киберпространством, цифровыми технологиями и технологиями. Это важный шаг в продвижении внешней политики США. Департамент будет работать над введением в действие и реализацией этих новых полномочий.

Украина

Соединенные Штаты, союзники и партнеры в течение многих лет инвестировали в наращивание потенциала Украины в киберпространстве, обеспечивая основу для более оперативной помощи в смягчении последствий атак и восстановлении после них. До полномасштабного вторжения России в Украину американские ведомства, включая Федеральное бюро расследований, Киберкомандование США и Агентство по кибербезопасности и безопасности инфраструктуры, делились киберразведданными с украинскими партнерами. С момента вторжения правительства Соединенных Штатов, Великобритании и ЕС предоставили более 100 миллионов долларов иностранной помощи в киберпространстве и позволили украинским агентствам получить доступ к услугам коммерческих компаний по кибербезопасности. В 2023 году США и девять близких партнеров учредили Таллиннский механизм — донорскую координационную группу, целью которой является быстрое и эффективное предоставление помощи в поддержку наиболее насущных потребностей Украины в области кибербезопасности.

Коста-Рика

После года неоднократных атак программ-вымогателей на правительственные сети Коста-Рики, которые повлияли на критически важные услуги, такие как здравоохранение, сбор налогов и таможня, и привели к чрезвычайной ситуации в стране, Соединенные Штаты объявили о пакете помощи в размере 25 миллионов долларов США для устранения немедленных критических киберуязвимостей, включая оборудование, программное обеспечение, лицензии и встроенную техническую поддержку. В сотрудничестве с Министерством науки, инноваций, технологий и телекоммуникаций Коста-Рики Соединенные Штаты помогли создать и оснастить централизованный центр управления безопасностью для

мониторинга, предотвращения, обнаружения, расследования и реагирования на киберугрозы. Соединенные Штаты также поддерживают среднесрочные и долгосрочные технические проекты и подготовку кадров, чтобы помочь Коста-Рике создать безопасную, устойчивую и устойчивую на местном уровне киберэкосистему.

Албания

В случае с Албанией после просьбы премьер-министра в июле 2022 года США оперативно развернули технические группы в ответ на разрушительную кибератаку, в ходе которой использовались программы-вымогатели и вредоносные программы-вайперы против сетей государственного сектора, в том числе некоторых из них, которые Албания определила как критически важную инфраструктуру. Правительство США и частный сектор возложили ответственность за атаку на Иран, а Госдепартамент координировал дипломатическую кампанию, которая включала санкции США и заявления НАТО и ЕС с осуждением. После этих более незамедлительных ответов Госдепартамент обратился к долгосрочному наращиванию потенциала, в том числе к оказанию помощи США гражданским и военным ведомствам на сумму более 50 миллионов долларов США для укрепления их сетей. Международные партнеры, такие как Великобритания и ЕС, также оказали помощь в области кибербезопасности. Агентства США, включая Государственный департамент, Федеральное бюро расследований, Киберкомандование США и Агентство по кибербезопасности и безопасности инфраструктуры, продолжают сотрудничать с албанскими кибервластями после последующих менее масштабных кибератак в 2023 и 2024 годах.

Заключение

Как отмечают в СНБ и НКС, 2020-е годы являются решающим десятилетием, и действия, предпринятые сейчас, сформируют контуры киберпространства, цифровых технологий и цифровой экономики на будущее. Реализуя эту стратегию, Государственный департамент будет работать с Конгрессом и межведомственными партнерами над оценкой существующих кибервластей и внесением поправок или созданием полномочий по мере необходимости, чтобы Госдепартамент мог идти в ногу с развивающимися кибер- и цифровыми технологиями.

Создание инновационных, безопасных и уважающих права цифровых экосистем — это процесс, который выйдет за рамки временной шкалы этой стратегии и, вероятно, будет характеризоваться прогрессом, паузами и разворотами. Тем не менее, появятся некоторые первые признаки, указывающие на то, что Соединенные Штаты, их союзники и партнеры движутся вперед.

Во-первых, Соединенные Штаты, союзники и партнеры, а также частный сектор и гражданское общество будут опираться на первые успехи Кодекса поведения G7 в Хиросиме, Указа Байдена-Харрис об ИИ и Саммита по безопасности ИИ в Великобритании. Мы придем к консенсусу в отношении руководящих принципов, способствующих инновациям и развитию ответственного ИИ, а также сделаем значительные инвестиции в создание знаний и инфраструктуры, необходимых для измерения, оценки и проверки передовых систем ИИ, в том числе путем создания Института безопасности ИИ США. Мы будем продвигать глобальные нормы ответственного и уважающего права человека использования технологий на основе ИИ.

Во-вторых, союзники и партнеры Соединенных Штатов вместе с частным сектором выработают общее понимание и общие принципы безопасности и надежности подводных кабелей, облачных сервисов и центров обработки данных, а также увеличат поддержку расширения доступа к облачным сервисам в странах с развивающейся экономикой.

В-третьих, Соединенным Штатам, их союзникам и партнерам удастся продвинуть в ООН более целенаправленные дискуссии по вопросам международной безопасности в киберпространстве. Эти дискуссии будут сосредоточены на том, как государства-члены могут работать вместе для реализации важнейших элементов рамочной программы ответственного

поведения государств, а также на наращивании потенциала всех государств для управления киберугрозами.

В-четвертых, Государственный департамент будет использовать средства Фонда киберпространства, цифровой связи и смежных технологий для быстрого и эффективного реагирования на инциденты и оказания киберпомощи, а также для долгосрочного наращивания потенциала и устойчивости. Эти стратегические инвестиции не только укрепят роль Соединенных Штатов как цифрового партнера, но и привлекут более крупные, самоокупаемые инвестиции принимающих стран в собственную кибербезопасность и цифровую трансформацию.

Двигаясь вперед, Соединенные Штаты будут стремиться к будущему, в котором киберпространство и цифровые технологии будут использоваться для содействия экономическому процветанию и инклюзивности, укрепления безопасности, поощрения и защиты прав человека и демократии, а также для решения транснациональных проблем. Государственный департамент будет укреплять и распространять цифровую солидарность на партнеров по всему миру. Соединенные Штаты признают необходимость совместной работы по согласованию подходов к данным и цифровому управлению, а также по содействию исследованиям, разработкам и внедрению критически важных и новых технологий. Соединенные Штаты стремятся стать предпочтительным партнером в области повышения кибербезопасности, повышения устойчивости, реагирования на злонамеренную киберактивность и восстановления после нее. Цифровая солидарность направлена на то, чтобы объединить людей и информацию, как никогда раньше, способствуя созданию более инклюзивного, безопасного, процветающего, уважающего права человека, безопасного и справедливого мира.