Отчет о ситуации в стране: Нидерланды и «публичное ядро интернета»

Алексей Трепыхалин и Вени Марковски
28 мая 2021 года
GE-008

ICANN

СОДЕРЖАНИЕ

Введение

Настоящий отчет посвящен национальным и международным инициативам в области интернета, предпринятым правительством Нидерландов. Это один из периодических отчетов о деятельности в конкретных странах, связанной с экосистемой интернета и миссии ICANN. Мониторинг этой деятельности выполняется для выполнения обязательств и обязанностей отдела по взаимодействию с правительствами и межправительственными организациями (GE) корпорации ICANN в области информирования всего сообщества ICANN о вопросах, представляющих важность для глобального единого функционально совместимого интернета и его системы уникальных идентификаторов.[1]

Как и в предыдущих документах GE, настоящий анализ основан на текстах первоисточников, касающихся политики в области интернета и интернет-технологий, таких как система доменных имен (DNS), IP-адреса, параметры протоколов и др. Кроме того, данная работа опирается на соответствующие тексты и заявления с изложением позиции правительства Нидерландов по этим вопросам в Организации Объединенных Наций (ООН). Это делается для того, чтобы у сообщества ICANN была необходимая информация для более полного понимания дискуссий, происходящих в ООН.

И, наконец, в данном отчете уделяется внимание одному термину, продвигаемому Нидерландами в частном и публичном пространствах — «публичное ядро интернета». В ООН этот термин используется в заявлениях, сделанных Нидерландами в рамках участия в деятельности Рабочей группы открытого состава Генеральной Ассамблеи ООН в сфере информатизации и телекоммуникаций в контексте международной безопасности (OEWG).[2] [3]

Для справки: история термина «публичное ядро»

За последние несколько лет термин «публичное ядро интернета» неоднократно упоминался в различных ситуациях. Ниже приведены лишь отдельные примеры его использования.

[1] План операционной деятельности и финансовый план ICANN, с. 47, корпорация ICANN, декабрь 2020 года, https://www.icann.org/en/system/files/files/draft-op-financial-plan-fy21-25-opplan-fy21-20dec19-en.pdf

[2] Ответ Королевства Нидерландов на предварительную версию проекта отчета OEWG, рабочей группы открытого состава, созданной Генеральной ассамблеей *[Kingdom of the Netherlands' response to the pre-draft report of the OEWG, General Assembly established an Open-Ended Working Group (OEWG)]*, 2020, https://front.un-arm.org/wp- content/uploads/2020/04/kingdom-of-the-netherlands-response-pre-draft-oewg.pdf

[3] Документ о позиции Нидерландов в отношении Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и Группы правительственных экспертов ООН по «продвижению ответственного поведения государств в киберпространстве в контексте международной безопасности *[Netherlands' position paper on the UN Open-ended Working Group "on Developments in the Field of Information and Telecommunications in the Context of International Security" and the UN Group of Governmental Experts "on Advancing responsible State behavior in cyberspace in the context of international security"],* Рабочая группа открытого состава, февраль 2020, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/letter-to-chair-of-oewg-kingdom-of-the-netherlands.pdf

В 2015 году Научный совет по государственной политике Нидерландов представил министру иностранных дел Нидерландов Берту Кундерсу отчет под названием «Публичное ядро интернета».[4]

В 2016 году Министерство иностранных дел Нидерландов провело консультативный семинар с представителями технического и некоммерческого сообществ. В ходе семинара были сделаны следующие заявления: «защита публичного ядра была определена как защита общей доступности основных функций по пересылке и присвоению имен в глобальном интернете».[5]

Нидерланды ввели этот термин в ООН в 2016–2017 гг. в Группе правительственных экспертов (GGE).[6] Поскольку GGE не выпустила согласованный отчет, неизвестно, попал бы этот термин в окончательный текст.[7]

В 2017 году правительство Нидерландов поддержало создание частной организации под названием Глобальная комиссия по стабильности в киберпространстве (GCSC).[8] В 2018 году GCSC опубликовала определение, в котором говорится, что фраза «публичное ядро интернета» включает «такие критически важные элементы инфраструктуры интернета, как маршрутизация и пересылка пакетов, системы присвоения имен и нумерации, криптографические механизмы безопасности и идентификации, средства передачи данных, программное обеспечение и дата-центры».[9]

[4] Dennis Broeders, The Public Core of the Internet. An International Agenda for Internet Governance *[Деннис Бредерс, Публичное ядро интернета. Международная повестка дня управления интернетом»]*, Научный совет по государственной политике Нидерландов, январь 2015 года, https://english.wrr.nl/publications/reports/2015/10/01/the-public-core-of-the-internet

[5] Dennis Broeders, Aligning the International Protection of 'the Public Core of the Internet' with State Sovereignty and National Security» *[Деннис Бредерс, Координация действий по международной защите публичного ядра интернета с обеспечением государственного суверенитета и национальной безопасности]*, Journal of Cyber Policy, том 2, выпуск 4, ноябрь 2017, стр. 369, https://www.researchgate.net/publication/321237654_Aligning_the_international_protection_of_'the_public_core_of_the_internet'_with_state_sovereignty_and_national_security

[6] Группа правительственных экспертов, Управление Организации Объединённых Наций по вопросам разоружения, май 2021 года, https://www.un.org/disarmament/group-of-governmental-experts/

[7] Fact Sheet: Developments In the Field of Information and Telecommunications in the Context of International Security *[Информационный листок: Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности]*, Управление Организации Объединённых Наций по вопросам разоружения, июль 2019 года, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf

[8] Создана Глобальная комиссия по стабильности в киберпространстве, Глобальная комиссия по стабильности в киберпространстве, 18 февраля 2017 года, https://cyberstability.org/news/launch-of-global-commission-on-the-stability-of-cyberspace/

[9] Definition of the Public Core, to Which the Norm Applies *[Определение понятия «публичное ядро», подлежащего применению нормы]*, Глобальная комиссия по стабильности в киберпространстве, май 2018 года, https://cyberstability.org/wp-content/uploads/2018/07/Definition-of-the-Public- Core-of-the-Internet.pdf

В 2017 году Министерство иностранных дел Нидерландов представило международную киберстратегию, , согласно которой, «учитывая природу киберпространства и нашу зависимость от него, необходимо проявлять сдержанность при осуществлении деятельности, которая может повлиять на это публичное ядро».[10] Одновременно в описании этой стратегии также отмечается, что «в максимально возможной степени ответственность за поддержание и развитие этого публичного ядра должна лежать на технологическом сообществе, а государство должно играть вспомогательную роль».

В 2017 и 2018 годах рабочая группа GCSC провела опрос экспертов по инфраструктуре связи и киберзащите «для оценки того, какие инфраструктуры требуют защиты в первую очередь».[11] В результате GCSC подготовила следующее определение «публичного ядра»: «системы маршрутизации и пересылки пакетов, присвоения имен и нумерации, криптографические механизмы безопасности и идентификации, а также физические средства передачи данных» (см. Приложение III).[12]

В 2019 году на конференциях ICANN64 и ICANN65 в Кобе и Марракеше соответственно, участники GCSC ввели в употребление термин «публичное ядро». Впервые этот термин обсуждался в Кобе на встрече Группы интересов интернет-провайдеров и провайдеров связи (ISPCP) Организации поддержки доменов общего пользования (GNSO).[13] В том же году в Марракеше GCSC представила проект своего отчета широкому интернет-сообществу в рамках своей информационно-просветительской деятельности. На конференции в Марракеше представитель Великобритании в Правительственном консультативном комитете (GAC) ICANN предупредил GCSC, что «введение такого термина, как публичное ядро, который не очень хорошо понимают или которому трудно дать определение, может создать еще больше проблем».[14]

[10] Министерство иностранных дел, Building Digital Bridges. International Cyber Strategy. Towards an Integrated International Cyber Policy *[Строительство цифровых мостов, международная киберстратегия для координированной политики в области международной стратегии кибербезопасности]*. Письмо парламенту, 2017 год, https://www.government.nl/documents/parliamentary-documents/2017/02/12/international-cyber-strategy

[11] Louk Faeson, Call to Protect the Public Core of the Internet *[Лук Фаэзон, «Призыв к защите публичного ядра интернета]*, Глобальная комиссия по стабильности в киберпространстве, декабрь 2017 года, https://cyberstability.org/category/front/

[12] Definition of the Public Core, to Which the Norm Applies *[Определение понятия «публичное ядро», подлежащего применению нормы]*, Глобальная комиссия по стабильности в киберпространстве, май 2018 года.

[13] Стенограмма совещания ISPCP, корпорация ICANN, март 2019, 15:15 JST, (стр. 22-23, 26), https://gnso.icann.org/sites/default/files/file/field-file-attach/transcript-gnso-ispcp-12mar19-en.pdf

[14] GAC: Совместное совещание с Глобальной комиссией по стабильности в киберпространстве (GCSC), корпорация ICANN, 27 июня 2019 года (начало в 22:39), https://icann.zoom.us/recording/share/yW2zWMtn2QzgJTmj0u3sh-zWa6-FuQel7V72gUoFfaewIumekTziMw?startTime=1561633270000

Использование термина «публичное ядро» при обсуждении вопросов кибербезопасности в Организации Объединенных Наций [15]

В 2020 году термин «публичное ядро» появился в некоторых документах, опубликованных на официальной веб-странице Рабочей группы открытого состава.[16]

В первой версии предварительного проекта доклада Председателя этот термин встречается в пункте 38: «Государства в ходе дискуссий и в письменных замечаниях также выдвигали предложения по «совершенствованию» и дальнейшему уточнению норм. В частности, поступили следующие предложения: государствам следует подтвердить свою приверженность международному миру и безопасности при использовании ИКТ; необходимо вновь заявить, что государства несут основную ответственность за сохранение безопасной, надежной среды ИКТ, которой можно доверять; необходимо защитить общедоступность и целостность публичного ядра интернета [...].[17]

Во второй версии доработанного предварительного проекта доклада Председателя этот термин встречается в пункте 42: «Государства также внесли предложения по усовершенствованию и дальнейшей разработке норм. Среди прочего поступили следующие предложения: государства должны подтвердить свою приверженность культуре сдержанности и международному миру и безопасности при использовании ИКТ; государства должны подтвердить, что они несут основную ответственность за поддержание безопасной, защищенной и вызывающей доверие среды ИКТ; и что общая доступность и целостность общественного ядра Интернета должны быть защищены[...]». [18]

[15] Прежде чем объяснить, где и как этот термин используется в рамках различных дискуссий в ООН, важно отметить, что, хотя этот термин существует в некоторых законодательных и политических актах, таких как Международная киберстратегия Нидерландов или Закон ЕС о кибербезопасности, у ООН нет практики брать формулировки из национальных законов и нормативных актов и использовать их непосредственно в своих итоговых документах.
[16] Рабочая группа открытого состава, Генеральная Ассамблея ООН, май 2021 года, https://www.un.org/disarmament/open-ended-working-group/
[17] Предварительный проект доклада Председателя, март 2020 года, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/03/200311-Pre-Draft-OEWG-ICT.pdf
[18] Предварительный проект доклада Председателя, май 2020 года, https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf

В своем вкладе в OEWG в феврале 2020 года Нидерланды выдвинули предложение о том, что вопрос защиты публичного ядра должен рассматриваться как специалистами OEWG, так и специалистами GGE. [19] Ряд других государств-членов также упомянули этот термин в своих материалах, включая Германию, Швейцарию и ЕС.[20,21,22] Он также упоминался в материалах других заинтересованных сторон, таких как 12 неправительственных организаций, корпорация Microsoft, Global Partners Digital и Общество Интернета.[23,24,25,26,27] Общество Интернета дало такое определение: «публичное ядро интернета включает в себя системы маршрутизации, присвоения имен и нумерации интернета (систему доменных имен), механизмы обеспечения безопасности и шифрования личности, а также кабели связи».

---

[19] Netherlands' position paper on the UN Open-ended Working Group "on Developments in the Field of Information and Telecommunications in the Context of International Security" and the UN Group of Governmental Experts "on Advancing responsible State behavior in cyberspace in the context of international security *[Документ с изложением мнений Нидерландов о Рабочей группе ООН открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и Группы правительственных экспертов ООН по «продвижению ответственного поведения государств в киберпространстве в контексте международной безопасности]*, Рабочая группа открытого состава, Генеральная ассамблея ООН, март 2020 года, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/letter-to-chair-of-oewg-kingdom-of-the-netherlands.pdf

[20] Initial 'Pre-Draft' of the Report of the OEWG On Developments in the Field of Information and Telecommunications in the Context of International Security and Non-Paper Listing Specific Language Proposals Under Agenda Item 'Rules, Norms and Principles' From Written Submissions Received Before 2 March 2020 *[Предварительный проект доклада Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и неофициальный перечень конкретных предложений относительно формулировок, связанных с пунктом повестки дня «Правила, нормы и принципы», поступивших в письменной форме по состоянию на 2 марта 2020 года]*, комментарии Германии, Рабочая группа открытого состава, Генеральная ассамблея ООН, апрель 2020 года, https://front.un-arm.org/wp-content/uploads/2020/04/20200401-oewg-german-written-contribution-to-pre-draft-report-1.pdf

[21] Постоянный представитель Надин Оливьери Лозано (Nadine Olivieri Lozano), Letter to the Chair of the UN Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security *[Письмо председателю Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности]*, Рабочая группа открытого состава, Генеральная ассамблея ООН, 9 апреля 2020 года, https://front.un-arm.org/wp-content/uploads/2020/04/20200409-switzerland-remarks-oewg-pre-draft.pdf

[22] Joint Comments from the EU and its Member States on the Initial 'Pre-Draft' Report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunication in the Context of International Security *[Совместные замечания ЕС и его государств-членов о Предварительном проекте доклада Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности]*, Рабочая группа открытого состава, Генеральная ассамблея ООН, май 2020 года, https://front.un-arm.org/wp-content/uploads/2020/05/eu-contribution-alignments-oewg.pdf

[23] Civil Society Perspectives on the "Initial Pre-Draft of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security *[Взгляд гражданского общества на «Предварительный проект доклада Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности]*, Рабочая группа открытого состава, Генеральная ассамблея ООН, апрель 2020 года, https://front.un-arm.org/wp-content/uploads/2020/04/cs-coordination-perspectives-on-oewg-pre-draft.pdf

[24] Ответ Global Partners Digital на предварительный проект доклада, Global Partners Digital, март 2020 года, https://front.un-arm.org/wp-content/uploads/2020/04/oewg-pre-draft-gpd-response-final.pdf

[25] Замечания Microsoft по Предварительному проекту доклада Рабочей группы открытого состава о кибербезопасности, Microsoft Inc., апрель 2020 года, https://front.un-arm.org/wp-content/uploads/2020/04/microsoft-response-to-draft-oewg-report.pdf и

[26] Ответ Общества Интернета на первоначальный предварительный отчет OEWG, https://front.un-arm.org/wp- content/uploads/2020/04/internet-society-response-pre-draft-report-of-oewg-04-14-20-en.pdf

[27] Protecting People In Cyberspace: The Vital Role Of The United Nations In 2020 *[Защита людей в киберпространстве: ключевая роль ООН в 2020 году]*, Microsoft Inc., апрель 2020 года, https://front.un-arm.org/wp-content/uploads/2020/04/protecting-people-in-cyberspace- december-2019.pdf

Использование этого термина не получило всеобщей поддержки. Китай, например, выразил сомнения в том, что этот термин должен быть включен в доклад Председателя, заявив: «Учитывая, что у нас ограниченное количество времени, следует избегать включения в отчет понятий, относительно которых еще не достигнут глобальный консенсус (таких как «публичное ядро»)».[28]

В марте 2020 года в неофициальном документе была приведена конкретная формулировка, предложенная Нидерландами: «Государственные и негосударственные субъекты не должны ни вести, ни сознательно разрешать деятельность, преднамеренно наносящую существенный ущерб общедоступности или целостности публичного ядра интернета и, следовательно, стабильности киберпространства». Это [может стать] руководством по реализации рекомендации 13(f) ГПЭ ООН 2015 года и, соответственно, также было бы отнесено к области действия рекомендации 13(g) ГПЭ ООН 2015 года».[29]

В декабре 2020 года в ходе неофициального "Кибер-диалога с участием многих заинтересованных сторон в поддержку продолжающейся дискуссии в Рабочей группе ООН открытого состава (OEWG) о развитии информационно-коммуникационных технологий (ИКТ) в контексте международной безопасности» представители GCSC и ISOC продолжили изучение целесообразности использования термина «публичное ядро».[30]

19 января 2021 года OEWG опубликовала *Нулевую версию проекта отчета*, в которой термин «публичное ядро» не упоминался.[31] То же самое произошло и в *Первой версии проекта отчета*, опубликованной 1 марта 2021 года.[32]

С 8 по 12 марта 2021 года OEWG провела свою третью предметную сессию, в ходе которой делегация Нидерландов предложила следующую исправленную формулировку о публичном ядре в «Нулевой версии проекта отчета»

«В соответствии с текстом о защите публичного ядра, который был включен в предварительный проект, учитывая сближение позиций относительно точной формулировки, мы предлагаем следующее. Мы хотели бы предложить изменить формулировку в последнем предложении параграфа 21 «целостность, функционирование и доступность» на [настоятельную потребность в защите] «технической инфраструктуры, необходимой для обеспечения общедоступности или целостности интернета». Это также касается параграфа 50. Кроме того, мы хотели бы упомянуть важность «защиты технической инфраструктуры, необходимой для обеспечения общедоступности или целостности интернета» в разделе «Вывод и рекомендация» *Правил, норм и принципов*.[33]

---

[28] Замечания Китая по Предварительному проекту доклада, Рабочая группа открытого состава, Генеральная ассамблея ООН, апрель 2020 года, https://front.un-arm.org/wp-content/uploads/2020/04/china-contribution-to-oewg-pre-draft-report-final.pdf

[29] Неофициальный перечень конкретных предложений относительно формулировок, связанных с пунктом повестки дня «*Правила, нормы и принципы»,* поступивших в письменной форме по состоянию на 2 марта 2020 года, OEWG, март 2020 года, https://unoda- web.s3.amazonaws.com/wp-content/uploads/2020/03/200311-OEWG-ICT-non-paper.pdf

[30] Обсудим кибербезопасность: правила, нормы и принципы, прямые трансляции, декабрь 2020 года (начало в 1:59:00), https://letstalkcyber.livecasts.eu/rules-norms-and-principles

[31] Проект предметного отчета [версия 0], Рабочая группа открытого состава, Генеральная ассамблея ООН, 19 января 2021 года, https://front.un-arm.org/wp-content/uploads/2021/01/OEWG-Zero-Draft-19-01-2021.pdf

[32] Предметный отчет [Первая версия]», 1 марта 2020 года, Рабочая группа открытого состава, Генеральная ассамблея ООН, https://front.un-arm.org/wp-content/uploads/2021/03/210301-First-Draft.pdf

[33] Нидерланды – письменные предложения относительно Нулевой версии проекта отчета OEWG, Рабочая группа открытого состава, Генеральная ассамблея ООН, февраль 2021 года, https://front.un-arm.org/wp-content/uploads/2021/02/Netherlands- OEWG-written-comments-to-zero-draft.pdf

Другие страны поддержали позицию Нидерландов, как устно, так и в письменных материалах в ходе сессии, а Великобритания отметила: «Мы выражаем благодарность Нидерландам за работу вместе с нами и другими лицами над уточнением их предложения по "публичному ядру" и приветствуем включение компромиссного текста».[34]

В двух случаях состоялись отдельные полуторачасовые неофициальные виртуальные обмены мнениями между заинтересованными сторонами OEWG, в ходе которых государства-члены выслушали мнения других заинтересованных сторон по содержанию первого проекта отчета. При выражении этих мнений в некоторых случаях упоминалось «публичное ядро», а именно в комментарии и заявлении GCSC, в которых выражается сожаление в связи с тем, что термин не был включен в согласованный отчет.[35,36,37]

В результате в итоговый отчет OEWG была включена следующая формулировка по этому вопросу в двух пунктах отчета, 18 и 26: [38]

«18. Государства пришли к выводу, что злонамеренная деятельность с использованием ИКТ против объектов критической инфраструктуры (CI) и критической информационной инфраструктуры (CII), обеспечивающих оказание населению социально значимых услуг, может привести к разрушительным последствиям в области безопасности, а также в экономической, социальной и гуманитарной областях. Хотя определение того, какие виды инфраструктуры считаются критически важными, является прерогативой каждого государства, такая инфраструктура может включать медицинские учреждения, финансовые службы, энергетику, водоснабжение, транспорт и санитарию. Направленная против CI и CII злонамеренная деятельность с использованием ИКТ, которая подрывает доверие к политическим и избирательным процессам, государственным учреждениям или оказывает негативное воздействие на общедоступность или целостность интернета, также является реальной и все более серьезной проблемой. Такой инфраструктурой может владеть или управлять частный сектор; она может использоваться совместно с другим государством или эксплуатироваться в разных государствах. Вследствие этого может возникать необходимость межгосударственного или государственно-частного сотрудничества для защиты ее целостности, работоспособности и доступности».

«26. Признавая необходимость защиты всех объектов критической инфраструктуры (CI) и критической информационной инфраструктуры (CII), обеспечивающих оказание населению социально значимых услуг, а также стремясь гарантировать общедоступность и целостность интернета, государства также пришли к выводу, что пандемия COVID-19 подчеркнула важность защиты инфраструктуры здравоохранения, в том числе медицинских служб и учреждений, путем введения норм, касающихся критической инфраструктуры, например тех, которые были утверждены на основе консенсуса в резолюции 70/237 Генеральной Ассамблеи ООН».[38]

---

[34] Замечания Соединенного Королевства о нулевой версии проекта отчета, Рабочая группа открытого состава, Генеральная ассамблея ООН, февраль 2020 года, https://front.un-arm.org/wp-content/uploads/2021/02/UK-submission-to- OEWG-ICTs-zero-draft-002.pdf

[35] Заявления межправительственных организаций (МПО) и неправительственных организаций (НПО), Рабочая группа открытого состава, Генеральная Ассамблея ООН, 2020 год, https://www.un.org/disarmament/open-ended-working-group/

[36] Комментарии GCSC по первой версии проекта предметного отчета Рабочей группы открытого состава ООН, Глобальная комиссия по стабильности в киберпространстве, 3 марта 2021, https://front.un- arm.org/wp-content/uploads/2021/03/GCSC-Submission-to-OEWG-First-Draft-Report-March-2021.pdf

[37] Комментарии GCSC по первой версии проекта отчета Рабочей группы открытого состава ООН, Глобальная комиссия по стабильности в киберпространстве, 12 марта 2021, https://front.un-arm.org/wp-content/uploads/2021/03/GCSC-Submission-to-OEWG-First-Draft-Report-March-2021.pdf

Заключение

Есть стороны, которые считают, что термин «публичное ядро» будет использоваться не только в контексте GGE и OEWG, но и за их пределами. Например, один из членов GCSC написал следующее о норме GCSC в области публичного ядра: «У этой нормы большой потенциал с точки зрения дальнейшего уточнения, и она может стать отправной точкой для составления нового типа международного соглашения, закрепляющего права и обязанности не только государств, но и негосударственных субъектов».[39]

Введение в документ ООН такого нового термина, как «публичное ядро», который «не получил глобального консенсуса»[40] и который не был определен ООН, может привести к возникновению различных толкований и конкурирующих определений, а также предоставить возможность ООН и другим МПО ссылаться на термин «публичное ядро» в собственной работе. Это, в свою очередь, может расширить сферу компетенции или деятельности этих МПО, включив в нее вопросы, которые в настоящее время входят в задачи и полномочия других многосторонних организаций.

Корпорация ICANN, через свою команду GE, будет и далее предоставлять информацию сообществу ICANN, когда заявления или предложения такого рода будут касаться технического управления Интернетом или миссии ICANN.

[38]Итоговая версия предметного доклада, Рабочая группа открытого состава, Генеральная Ассамблея ООН, 10 марта 2021 года, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

[39] Wolfgang Kleinwächter, Advancing Cyberstability: Protect the Public Internet Core and Improve Cyber Hygiene *[Вольфганг Клайнвахтер, Продвижение киберстабильности: защита публичного ядра интернета и повышение кибергигиены]*, CircleID, ноябрь 2019 года, https://www.circleid.com/posts/20191124_cyberstability_protecting_public_internet_core_and_cyber_hygiene/

[40] Заявление Китая о первоначальном предварительном проекте отчета OEWG, Рабочая группа открытого состава, Генеральная ассамблея ООН, апрель 2020 года, https://front.un-arm.org/wp-content/uploads/2020/04/china- contribution-to-oewg-pre-draft-report-final.pdf

Приложение I.

Международная стратегия кибербезопасности

В 2017 году правительство Нидерландов заявило, что, публикуя Международную киберстратегию, оно «выполняет обещание, данное в своем ответе на консультативные отчеты Консультативного совета по международным делам (AIV) (‘The Internet: A Global Free Space with Limited State Control’) и Научного совета по государственной политике (WRR) (‘The Public Core of the Internet’).”[41]

В этом документе, среди прочего, мы отмечаем следующие заявления:

- В пункте 2.4: «Экономические и социальные преимущества, связанные с интернетом, требуют надежного, предсказуемого, стабильного и безопасного функционирования "публичного ядра" интернета. Это ядро обладает элементами международного общественного блага, которое выходит за рамки индивидуальных суверенных и частных интересов. Нидерланды признают, что, учитывая природу киберпространства и нашу зависимость от него, необходимо проявлять сдержанность при осуществлении деятельности, которая может повлиять на это публичное ядро. В максимально возможной степени ответственность за поддержание и развитие этого публичного ядра должна лежать на технологическом сообществе, а государство должно играть вспомогательную роль».[42]

- В пункте 4.2: «Учитывая глобальные общественные интересы, связанные с интернетом, правительство также работает над признанием ядра интернета международным общественным благом. Нидерланды признают, что, учитывая природу киберпространства и зависимость от него, необходимо проявлять сдержанность при осуществлении деятельности, способной повлиять на это публичное ядро. Нидерланды работают над развитием и продвижением принятия международных норм и правил поведения, и с этой целью они представили предложение Группе правительственных экспертов ООН (ГПЭ ООН) по достижениям в области информации и телекоммуникаций в контексте международной безопасности».[43]

[41] Министерство иностранных дел, Нидерланды, «Building Digital Bridges, International Cyber Strategy Towards an integrated international cyber policy» *[Строительство цифровых мостов, международная киберстратегия для координированной политики в области международной стратегии кибербезопасности]*, письмо к парламенту, 2017 год https://www.government.nl/documents/parliamentary-documents/2017/02/12/international-cyber-strategy

[42] Министерство иностранных дел, Нидерланды, Building Digital Bridges, International Cyber Strategy Towards an integrated international cyber policy *(Строительство цифровых мостов, международная киберстратегия для координированной политики в области международной стратегии кибербезопасности]*, письмо к парламенту, 2017 год, пункт 2.4, принцип 4.

[43] Министерство иностранных дел, Нидерланды, Building Digital Bridges, International Cyber Strategy Towards an integrated international cyber policy *[Строительство цифровых мостов, международная киберстратегия для координированной политики в области международной стратегии кибербезопасности]*, письмо к парламенту, 2017 год , пункт 4.2.

Приложение II.

Отчет Консультативного совета по международным делам (AIV)

В отчете за 2014 год, «Интернет: глобальное свободное пространство с ограниченным государственным контролем», Консультативный совет по международным делам (AIV) признал, что «система адресации и доменных имен, которые имеют огромное коммерческое значение, также должны рассматриваться как элемент управления интернетом».[44]

[44] The Internet: A Global Free Space with Limited State Control *[Интернет: глобальное свободное пространство с ограниченным государственным контролем]*, Консультативный совет по международным делам, ноябрь 2014 года, стр. 48, https://www.advisorycouncilinternationalaffairs.nl/documents/publications/2014/12/01/the-internet

Приложение III.

Определение понятия «публичное ядро»

Следующие составляющие (маршрутизация и пересылка пакетов, системы присвоения имен и нумерации, криптографические механизмы безопасности и идентификации, физические средства передачи данных) более подробно описаны в тексте определения публичного ядра интернета, принятом GCSC в мае 2018 года в Братиславе: [45]

«**Маршрутизация и пересылка пакетов** включают, среди прочего: оборудование, средства, информацию, протоколы и системы, которые содействуют передаче пакетных сообщений от источника к месту назначения. Сюда входят пункты обмена интернет-трафиком (физические объекты, где генерируется пропускная способность интернета) и пиринговые и основные маршрутизаторы крупнейших сетей, которые делают эту пропускную способность доступной пользователям. Сюда также входят системы, необходимые для обеспечения подлинности маршрутизации и защиты сети от неправомерного поведения и разработка, производство и цепочка поставок оборудования, используемого для вышеуказанных целей. Сюда также относится целостность самих протоколов маршрутизации и процессов их разработки, стандартизации и обслуживания.

Системы присвоения имен и нумерации включают, среди прочего: системы и информацию, используемые в работе системы доменных имен интернета, включая регистратуры, DNS-серверы, содержимое зон, инфраструктуру и процессы, такие как DNSSEC, используемые для криптографической подписи записей, и информационные службы WHOIS для корневой зоны, иерархии обратных адресов, национальных доменов верхнего уровня, географических и интернационализированных доменов верхнего уровня, а также для новых и невоенных доменов общего пользования (верхнего уровня). Сюда входят часто используемые публичные рекурсивные DNS-резолверы. Они включают в себя системы Администрации адресного пространства Интернет и региональных интернет-регистратур, которые обеспечивают и поддерживают уникальное распределение IP-адресов, номеров автономных систем и идентификаторов Интернет-протокола. Сюда также относятся сами протоколы присвоения имен и нумерации и совокупность процессов стандартизации и результатов разработки и поддержания протоколов.

Криптографические механизмы безопасности и идентификации включают, среди прочего: криптографические ключи, которые используются для аутентификации пользователей и устройств и обеспечения безопасности интернет-транзакций, а также оборудование, средства, информация, протоколы и системы, которые позволяют производить, передавать, использовать и исключать эти ключи. Сюда входят серверы ключей PGP, центры сертификации и их инфраструктура открытых ключей, DANE (аутентификация именованных объектов на базе DNS) и поддерживающие эту процедуру протоколы и инфраструктура, механизмы отзыва сертификатов и журналы прозрачности, менеджеры паролей и аутентификаторы доступа в роуминге. Они также включают в себя целостность процессов стандартизации и результатов разработки и обслуживания криптографических алгоритмов и протоколов, а также разработку, производство и цепочку поставок оборудования, используемого для реализации криптографических процессов.

[45] Definition of the Public Core, to Which the Norm Applies *[Определение понятия «публичное ядро», подлежащего применению нормы]*, Глобальная комиссия по стабильности в киберпространстве, май 2018 года.

Физические средства передачи включают, среди прочего: физические кабельные системы и установки для проводной связи, обслуживающие население, будь то волокно или медь. Сюда входят наземные и подводные кабели, а также наземные станции, дата-центры и другие физические объекты, которые их поддерживают. Они включают в себя вспомогательные системы передачи, регенерации сигнала, разветвления, мультиплексирования и выделения сигнала из шумов. Подразумевается, что сюда входят кабельные системы, обслуживающие регионы или население, но не те, которые обслуживают клиентов отдельных компаний. Некоторые эксперты считают, что гораздо больше категорий инфраструктуры интернета и ИКТ заслуживают защиты, поэтому в будущем это определение может быть расширено».