



Генеральная Ассамблея

Distr.: General
17 August 2022
Russian
Original: English

Семьдесят седьмая сессия

Пункт 69 b) предварительной повестки дня*

**Поощрение и защита прав человека: вопросы
прав человека, включая альтернативные подходы
в деле содействия эффективному осуществлению
прав человека и основных свобод**

Односторонние санкции в киберпространстве: тенденции и проблемы**

Записка Генерального секретаря

Генеральный секретарь имеет честь препроводить Генеральной Ассамблее доклад Специального докладчика по вопросу о негативном воздействии односторонних принудительных мер на осуществление прав человека Елены Довгань, представленный в соответствии с резолюцией [76/161](#) Ассамблеи и резолюциями [27/21](#) и [45/5](#) Совета по правам человека.

* [A/77/150](#).

** Настоящий доклад был представлен после установленного срока, с тем чтобы включить в него самую последнюю информацию.



**Доклад Специального докладчика по вопросу о негативном
воздействии односторонних принудительных мер на
осуществление прав человека Елены Довгань**

Резюме

В настоящем докладе Специальный докладчик по вопросу о негативном воздействии односторонних принудительных мер на осуществление прав человека Елена Довгань представляет обзор и оценку развития кибертехнологий и их влияния на применение односторонних санкций, оценивает законность и гуманитарные последствия мер, принимаемых государствами и региональными организациями в отношении злонамеренной деятельности в киберпространстве, и уделяет особое внимание блокированию доступа к веб-страницам и программному обеспечению.

I. Введение

1. Настоящий доклад представляется Генеральной Ассамблее в соответствии с ее резолюцией 76/161 и резолюциями 27/21 и 45/5 Совета по правам человека, в которых Специальному докладчику по вопросу о негативном воздействии односторонних принудительных мер на осуществление прав человека Елене Довгань было предложено, в частности, собрать всю информацию, касающуюся негативного воздействия односторонних принудительных мер на осуществление прав человека; изучить соответствующие тенденции, события и проблемы; и выработать руководящие принципы и рекомендации относительно путей и средств предотвращения, минимизации и устранения их негативного воздействия на права человека; а также привлечь внимание Ассамблеи, Совета и Верховного комиссара Организации Объединенных Наций по правам человека к соответствующим ситуациям и случаям.
2. Специальный докладчик отметила ускоряющееся расширение использования односторонних санкций, касающихся киберсредств или относящихся к киберпространству, что приводит, в частности, к новым толкованиям понятия односторонних санкций. Признавая неоднозначный характер понятия «киберсанкции», она делает попытку определить, как развитие кибертехнологий повлияло на применение односторонних санкций отдельными государствами и как это отразилось на правах человека. Настоящий доклад содержит обзор и оценку: расширения односторонних санкций в киберпространстве; способов реагирования государств на «злонамеренную» деятельность, и юридические проблемы, связанные с таким реагированием; развития национального законодательства; гуманитарных последствий вводимых мер; предотвращения доступа к банковским услугам онлайн; кампаний по диффамации и угрозы санкций в рамках санкционных режимов; блокированию доступа к онлайн-платформам и услугам; и другой санкционной и связанной с санкциями деятельности в киберсфере.
3. Для целей настоящего доклада Специальный докладчик обратилась к государствам, специализированным учреждениям Организации Объединенных Наций, региональным организациям, правозащитным учреждениям, гражданскому обществу, ученым, исследовательским институтам и другим лицам с призывом представить материалы об односторонних санкциях в киберпространстве¹. Были получены ответы от правительств Беларуси, Зимбабве, Ирана (Исламская Республика), Кубы, Российской Федерации и Сирийской Арабской Республики. Кроме того, были получены ответы от страновой группы Организации Объединенных Наций в Сирийской Арабской Республике и ряда неправительственных организаций, организаций гражданского общества, коммерческих предприятий, ученых и заинтересованных лиц. Специальный докладчик выражает свою признательность всем респондентам.
4. Специальный докладчик стремится согласовать использование термина «киберсанкции» с тем, как традиционно определяются санкции, то есть исходя из используемых инструментов (экономические, финансовые или военные) или цели (секторальные или целевые). Она также отмечает, что любая ссылка на существование разрешения на введение киберсанкций не имеет под собой оснований в международном праве.
5. Специальный докладчик признает наличие многочисленных сообщений об отключениях Интернета и ограничениях доступа к Интернету, введенных правительствами. Однако этот вопрос не относится к сфере охвата мандата. Как

¹ Призыв к представлению материалов размещен на странице www.ohchr.org/en/calls-for-input/calls-input/call-input-reports-secondary-sanctions-civil-and-criminal-penalties.

следствие, в настоящем докладе Специальный докладчик уделяет особое внимание связанному с кибертехнологиями аспекту использования односторонних санкций государствами и региональными организациями и чрезмерному соблюдению таких санкций.

6. Специальный докладчик подчеркивает, что данная оценка односторонних санкций в киберпространстве не должна рассматриваться как основание для их легализации или узаконивания. Любые односторонние меры без разрешения Совета Безопасности или с чрезмерным выполнением такого разрешения, которые не могут быть квалифицированы как ответные ограничения или контрмеры, являются незаконными с точки зрения международного права и представляют собой односторонние принудительные меры, которые были осуждены в многочисленных резолюциях Совета по правам человека и Генеральной Ассамблеи. Развитие кибертехнологий приводит к необходимости оценки этих новых видов мер с точки зрения их законности.

II. «Злонамеренное» использование кибертехнологий как основание для введения односторонних санкций

7. Специальному докладчику известно об изменениях и сложностях, которые кибертехнологии приносят во все сферы жизни. Она также признает, что киберактивность частных субъектов может представлять угрозу для поддержания международного мира и безопасности², представляя собой трансграничные преступления, включая международный терроризм³; военные преступления, преступления против человечности или геноцид⁴; враждебную пропаганду; диффамацию⁵; или враждебность по отношению к правительствам, компаниям или отдельным лицам. Она признает, что при определенных условиях кибероперация может представлять собой вооруженное нападение или часть вооруженного нападения⁶ или быть частью военной операции в ходе немеждународного военного конфликта⁷.

8. Специальный докладчик подчеркивает, что по состоянию на июль 2022 года Совет Безопасности ввел целевые санкции в отношении злонамеренной активности с использованием киберсредств только один раз — против лиц и организаций в Йемене, ответственных за атаки с использованием беспилотных

² Резолюция 2462 (2019) Совета Безопасности, преамбула и пп. 19 и 21; резолюция 2419 (2018) Совета Безопасности, преамбула; резолюция 2490 (2019) Совета Безопасности, преамбула; резолюция 72/246 Генеральной Ассамблеи, пп. 7–8; Управление Организации Объединенных Наций по наркотикам и преступности, *Использование Интернета в террористических целях* (Вена, 2012 год), стр. 3–14 и 32–35; и документ A/70/174, п. 3.

³ Maura Conway, “Determining the role of the Internet in violent extremism and terrorism: six suggestions for progressing research”, *Studies in Conflict and Terrorism*, vol 40, No. 1 (2017) and Ines von Behr and others, *Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism*, online edition (RAND Corporation, 2013).

⁴ Резолюция 2490 (2019) Совета Безопасности, преамбула.

⁵ Eric de Brantandere, “Propaganda”, *Max Planck Encyclopedia of Public International Law*.

⁶ International Committee of the Red Cross (ICRC), Commentary of 2016 on article 2 of the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, paras. 253–256, URL: <https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=BE2D518CF5DE54EAC1257F7D0036B518>.

⁷ ICRC, Commentary of 2016 on article 3 of the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, paras. 436–437, URL: <https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=BA341028EBFF1E8C12563CD00519E66>.

летательных аппаратов и беспилотных катеров⁸. Во всех остальных случаях Совет Безопасности ссылался на основное обязательство государств по пресечению террористической деятельности в киберпространстве; обеспечению гарантии безопасности своих граждан перед лицом терроризма, в том числе путем контроля за информационными потоками; контролю за операциями с криптовалютой с целью предотвращения отмывания денег и финансирования терроризма⁹; контролю за информацией о пассажирах от разных авиакомпаний¹⁰; расследованию преступлений террористической направленности. Организация по безопасности и сотрудничеству в Европе (ОБСЕ) ссылается в таких случаях на обязательство государств гарантировать соблюдение всех стандартов надлежащей правовой процедуры¹¹.

9. В то же время Специальный докладчик отмечает отсутствие общего понимания термина «злонамеренный» применительно к киберактивности и его произвольное использование государствами¹². Она подчеркивает, что возможные ответы на злонамеренную деятельность в киберпространстве не могут иметь общий характер и что они зависят от квалификации каждого действия.

10. Специальный докладчик отмечает, что государственная практика введения санкций в ответ на реальную или предполагаемую злонамеренную киберактивность довольно обширна. В частности, Исполнительный приказ Соединенных Штатов Америки № 13694 от 1 апреля 2015 года с поправками, внесенными более поздними документами¹³, ввел перечень подпадающих под санкции действий, совершенных с использованием кибертехнологий¹⁴, который включал, в частности, атаки на критически важную инфраструктуру, вмешательство в избирательный процесс¹⁵, дестабилизацию работы сети или эксплуатации компьютерных систем, а также незаконное присвоение финансовых средств и личной информации. Впоследствии в него были добавлены вирусные атаки, приводящие к значительным разрушениям, предотвращение доступа к системам¹⁶, получение несанкционированного доступа к инфраструктуре выборов и предвыборных кампаний, скрытое распространение пропаганды и дезинформации¹⁷,

⁸ Резолюция Совета Безопасности 2140 (2014), пп. 11–19; резолюция Совета Безопасности 2216 (2015), пп. 14–19; и S/2021/79, пп. 62–70.

⁹ Резолюция Совета Безопасности 2462 (2019), п. 19.

¹⁰ Резолюция Совета Безопасности 2482 (2019), п. 15 с).

¹¹ OSCE Decision No. 7/06 of 5 December 2006 on countering the use of the Internet for terrorist purposes, document MC.DEC/7/06, and OSCE, “Executive summary of regional workshop on countering the use of the Internet for terrorist purposes for judges, prosecutors and investigators from South Eastern Europe”, 8 February 2017, URL: www.osce.org/files/f/documents/7/e/299091.pdf.

¹² Martha Finnemore and Duncan B. Hollis, “Beyond naming and shaming: accusations and international law in cybersecurity”, *European Journal of International Law*, vol. 31, No. 3 (2020).

¹³ Например, Соединенные Штаты, Исполнительный приказ № 13757 от 28 декабря 2016 года о принятии дополнительных мер по ликвидации чрезвычайной ситуации в стране в отношении значительной злонамеренной кибернетической деятельности.

¹⁴ Соединенные Штаты, Исполнительный приказ № 13694 от 1 апреля 2015 года о блокировке доступа к собственности определенных лиц, осуществляющих значительную злонамеренную кибернетическую деятельность. См. также Silvina M. Romano, “Psychological war reloaded: cyber-sanctions, Venezuela and geopolitics”, *Revista Internacional de Pensamiento Político*, vol. 12 (2017).

¹⁵ United States, Office of Foreign Assets Control, “Cyber-related sanctions program”, updated 3 July 2017, URL: <https://home.treasury.gov/system/files/126/cyber.pdf>.

¹⁶ Соединенные Штаты, Закон о противодействии российскому влиянию в Европе и Евразии от 2017 года, с поправками, пункт 224.

¹⁷ Соединенные Штаты, Исполнительный приказ № 13848 от 12 сентября 2018 года о введении определенных санкций в случае иностранного вмешательства в выборы в Соединенных Штатах.

усилия по подрыву демократических институтов в Соединенных Штатах и на территориях их союзников и партнеров, усилия по участию в злонамеренной кибернетической деятельности против Соединенных Штатов и их союзников и партнеров и содействию ей, усилия по поддержке и использованию транснациональной коррупции для влияния на иностранные правительства, а также усилия по осуществлению экстерриториальной деятельности, направленной против диссидентов или журналистов¹⁸.

11. Как сообщается, в период 2011–2021 годов Соединенные Штаты включили в перечень 303 физических и юридических лица из 10 государств в связи с различными видами злонамеренной активности с использованием киберсредств¹⁹. Например, в связи с вмешательством в выборы в список были включены два государственных органа, 46 граждан и 13 компаний Российской Федерации и Украины²⁰.

12. Специальный докладчик отмечает, что некоторые из этих мер принимаются Соединенными Штатами в связи с выполнением резолюций Совета Безопасности в отношении Корейской Народно-Демократической Республики²¹, чтобы пресечь попытки Корейской Народно-Демократической Республики использовать кибертехнологии для обхода санкций Совета Безопасности и дополнительных санкций Соединенных Штатов²².

13. В своем руководстве от 2020 года по киберугрозе, исходящей от Корейской Народно-Демократической Республики, Соединенные Штаты ссылаются на подрывную или разрушительную киберактивность, затрагивающую важнейшие объекты инфраструктуры Соединенных Штатов. Такая деятельность может преследоваться Соединенными Штатами, и могут применяться вторичные санкции²³. Соединенные Штаты также предлагают денежное вознаграждение за информацию, которая приведет к нарушению работы финансовых механизмов лиц, занимающихся определенной деятельностью, поддерживающей Корейскую Народно-Демократическую Республику, включая отмывание денег, уклонение от санкций и киберпреступность²⁴.

14. Специальный докладчик отмечает, что группа экспертов, созданная Советом Безопасности²⁵, обсудила вопрос об обходе Корейской Народно-Демократической Республикой финансовых санкций с помощью киберсредств²⁶ и

¹⁸ Соединенные Штаты, Исполнительный приказ № 14024 от 15 апреля 2021 года о блокировке доступа к собственности в отношении определенной вредной иностранной деятельности правительства Российской Федерации.

¹⁹ Jason Bartlett and Megan Ophel, "Sanctions by the numbers: spotlight on cyber sanctions", Center for a New American Security, 4 May 2021; список документов Соединенных Штатов, касающихся санкций, принятых в отношении злонамеренной активности с использованием киберсредств до 2020 года, доступен на сайте <https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/sanctions-related-to-significant-malicious-cyber-enabled-activities>; и Allison Peters and Pierce MacConaghy, "Unpacking US cyber sanctions" *Third Way*, 2021, annex 1.

²⁰ Congressional Research Service, "U.S. sanctions on Russia", updated 18 January 2022, URL: <https://sgp.fas.org/crs/row/R45415.pdf>.

²¹ См., например, резолюции 1718 (2006) и 2397 (2017) Совета Безопасности.

²² Tanya Chepkova, "North Korea committing cybercrimes to avoid US sanctions", Be in Crypto, 3 June 2019 and United States, Department of the Treasury, "Guidance on the North Korean cyber threat", cyber threat advisory, April 2020.

²³ United States, Department of the Treasury, "Guidance on the North Korean cyber threat", p. 8.

²⁴ См. официальный сайт правительства Соединенных Штатов «Вознаграждение за помощь правосудию», URL https://rewardsforjustice.net/english/about-rfj/north_korea.html.

²⁵ См. резолюцию Совета Безопасности 1874 (2009), пункт 26, и резолюцию Совета Безопасности 2515 (2020), пункт 1.

²⁶ S/2019/691, пункты 57–71 и S/2021/211, пункты 126–129.

рекомендовала Совету Безопасности рассмотреть возможность учета этой ситуации в любых будущих санкциях²⁷.

15. С 2019 года Европейский союз и Соединенное Королевство Великобритании и Северной Ирландии применяют меры, касающиеся серьезных или потенциальных кибератак, под которыми понимаются действия, связанные с получением доступа к информационным системам, вмешательством в работу информационных систем, искажением данных или перехватом данных²⁸. Под кибератаками, представляющими угрозу для Европейского союза, подразумевается широкий спектр действий, включающий «атаки, совершенные в отношении его учреждений, органов, подразделений и учреждений, его делегаций в третьих странах или международных организациях, его операций и миссий по общей политике безопасности и обороны и его специальных представителей». Европейский союз и Соединенное Королевство ввели запреты на выдачу виз и въезд в страну, а также потребовали заморозить активы включенных в список лиц или отказать им в предоставлении активов или средств²⁹.

16. В результате в 2020 году восемь физических и четыре юридических лица из Китая, Корейской Народно-Демократической Республики и Российской Федерации были включены в список, поскольку считались оказавшими поддержку или участвовавшими в кибератаках или попытках кибератак, включая попытку кибератак на Организацию по запрещению химического оружия и кибератаки, известные как WannaCry и NotPetya, а также кибератаку, известную как Operation Cloud Horrer, и участвовавшими в кибератаках со значительными последствиями, представлявшими внешнюю угрозу для Европейского союза или его государств-членов, в частности, в кибератаке на федеральный парламент Германии в апреле и мае 2015 года³⁰.

17. После решения Великобритании покинуть Европейский союз, или «брекзита», Соединенное Королевство приняло постановление о киберсанкциях³¹, предусматривающее односторонние санкции против тех же лиц, указанных в списке Европейского союза³². Специальный докладчик с сожалением отмечает, что при разработке этого постановления не была проведена ни оценка законности, ни оценка гуманитарного воздействия³³.

18. Поправки, внесенные в Закон об автономных санкциях Австралии в 2021 году, предусматривают возможность введения односторонних санкций в ответ на «злонамеренную деятельность в киберпространстве»³⁴. По состоянию на июль 2022 года никаких санкций такого типа Австралия не вводила.

²⁷ S/2019/691, рекомендации 8–11; и S/2020/151, рекомендации содержатся в приложении 73.

²⁸ Council of the European Union Regulation No. 2019/796 of 17 May 2019 concerning restrictive measures against cyberattacks threatening the European Union or its member States, art. 1 (5–6). До 31 декабря 2020 года Великобритания применяла киберсанкции Европейского союза.

²⁹ Council of the European Union Regulation No. 2019/796 of 17 May 2019 concerning restrictive measures against cyberattacks threatening the European Union or its member States.

³⁰ Council of the European Union Implementing Regulation No. 2020/1125.

³¹ United Kingdom, Cyber (Sanctions) (EU Exit) Regulations 2020 No. 597 of 17 June 2020, URL: www.legislation.gov.uk/ukxi/2020/597/made.

³² Iryna Bogdanova and María Vázquez Callo-Müller, “Unilateral cyber sanctions: between questioned legality and normative value”, *Vanderbilt Journal of Transnational Law*, vol. 54 (2021).

³³ См. United Kingdom, Explanatory Memorandum to the Cyber (Sanctions) (EU Exit) Regulations 2020 No. 597, URL: www.legislation.gov.uk/ukxi/2020/597/pdfs/ukxiem_20200597_en.pdf.

³⁴ Australia, Autonomous Sanctions Amendment (Magnitsky-style and Other Thematic Sanctions) Act 2021, No. 128, 2021, para. 4, URL: www.legislation.gov.au/Details/C2021A00128.

19. Специальный докладчик с озабоченностью отмечает новую тенденцию среди ряда государств отзываться лицензии у средств массовой информации; удалять товары, услуги или контент в Интернете; или предусматривать уголовную или гражданскую ответственность за связанную с санкциями деятельность в киберпространстве.

20. В частности, ей известно об обсуждении Европейским союзом Закона о цифровых услугах, который направлен на установление «правил удаления незаконных товаров, услуг или контента в Интернете» и обязательств платформ «принимать учитывающие риски действия для предотвращения злоупотреблений их системами», дополняющие Европейский план действий по демократии³⁵. Этот План предусматривает меры по содействию проведению свободных и справедливых выборов, укреплению свободы средств массовой информации и противодействию дезинформации. Под последним понимается ложный или вводящий в заблуждение контент, распространяемый с вредоносным намерением или без него, а также информация для оказания влияния на операции и иностранное вмешательство в информационное пространство³⁶. В руководстве по укреплению кодекса по борьбе с дезинформацией, представленном Европейской комиссией в 2021 году, дезинформация понимается чрезвычайно широко и определяется как включающая дезинформацию, ложную информацию, действия по информационному влиянию и иностранное вмешательство в информационное пространство, в том числе со стороны иностранных субъектов, в тех случаях, когда манипулирование информацией используется с целью нанесения значительного общественного вреда³⁷.

21. Специальному докладчику также известно, что это фактически позволяет осуществлять публичное наблюдение за социальными сетями и требовать от платформ удаления соответствующих твитов, блогов и личных сообщений. Между тем, общественный вред также рассматривается очень широко и определяется как «реальное и предсказуемое негативное воздействие на общественное здоровье, общественную безопасность, гражданскую дискуссию, политическое участие и равенство»³⁸. Крупным платформам следует учитывать «возможное негативное воздействие системных рисков на общество и демократию, таких как дезинформация или манипулятивная и оскорбительная деятельность»³⁹, что трактуется как включающее в себя «распространяемые государством ложные сведения»⁴⁰.

22. Специальный докладчик с обеспокоенностью отмечает, что указанная тенденция прослеживается в недавних санкциях, введенных Австралией,

³⁵ European Commission, “Europe fit for the digital age: Commission proposes new rules for digital platforms”, 15 December 2020, URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2347.

³⁶ European Commission, “On the European democracy action plan”, communication from the Commission to the European Parliament, the Council, the European Economic And Social Committee and the Committee of the Regions, COM(2020) 790 final.

³⁷ European Commission, “European Commission guidance on strengthening the code of practice on disinformation”, communication from the Commission to the European Parliament, the Council, the European Economic And Social Committee and the Committee of the Regions, COM(2021) 262 final, para. 3.2.

³⁸ European Commission, “Proposal for a regulation of the European Parliament and of the Council on a single market for digital services (Digital Services Act) and amending Directive 2000/31/EC”, para. 63.

³⁹ Ibid., para. 68.

⁴⁰ Zach Meyers, “Will the Digital Services Act save Europe from disinformation?” Centre for European Reform, 21 April 2022.

Великобританией⁴¹, Канадой⁴² и Соединенными Штатами, а также Европейским союзом, которые в 2022 году отозвали разрешения у некоторых средств массовой информации Российской Федерации («Спутник» и «РТ»), ссылаясь в качестве оснований на политику этих средств массовой информации по отражению позиции Российской Федерации по конфликту на Украине, дезинформацию, иностранное вмешательство и действия по оказанию влияния, «пропагандистские действия, направленные на гражданское общество в Европейском союзе и соседних странах, серьезно искажающие факты и манипулирующие ими», и действия, представляющие «значительную и прямую угрозу общественному порядку и безопасности Европейского союза»⁴³. Та же тенденция прослеживается и в отношении статуса многих журналистов государственных средств массовой информации. Определенные ограничения были введены и в других странах. Некоторые страны Европейского союза ограничили доступ к более широкому списку телеканалов Российской Федерации⁴⁴.

23. Специальный докладчик обеспокоен тем, что, хотя необходимость соблюдения свободы выражения мнений признается в вышеупомянутых документах, ограничения оправдываются тем, что эти средства массовой информации контролируются Российской Федерацией, но при этом не проводится оценка в соответствии со статьями 19 и 20 Международного пакта о гражданских и политических правах.

24. В то же время, последующее решение Российской Федерации ограничить вещание и онлайн-доступ к Би-Би-Си, «Голосу Америки», «Дойче велле», «Медузе» и другим средствам массовой информации было осуждено Европейским союзом как ограничение свободы слова⁴⁵, несмотря на существующий доклад об использовании непроверенной информации в сообщениях о конфликте на Украине⁴⁶. Соединенные Штаты представили аналогичные возражения после того, как Российская Федерация заблокировала доступ к «Инстаграму» и «Фейсбуку» из-за уголовного дела против компании «Мета» по статьям 205.1 и 280 Уголовного кодекса Российской Федерации по обвинению в содействии экстремистской и террористической деятельности⁴⁷.

III. Санкции на торговлю и доступ, касающиеся программного обеспечения и онлайн-платформ

25. Специальный докладчик принимает во внимание сообщения о росте проблем с доступом к программному обеспечению и онлайн-платформам. Торговля программным обеспечением часто ограничивается в рамках режима санкций. В

⁴¹ France 24, “YouTube blocks Russian state-funded media, including RT and Sputnik, around the world” 12 March 2022 и Rebecca Alter, “RT America shuts down amid Russian State-media bans”, Vulture, 6 March 2022.

⁴² BBC, “RT: Russian-backed TV news channel disappears from UK screens”, 3 March 2022.

⁴³ Council of the European Union Regulation No. 2022/350 of 1 March 2022 amending Regulation No. 833/2014 concerning restrictive measures in view of Russia’s actions destabilising the situation in Ukraine, and Council of the European Union Decision No. 2022/351 of 1 March 2022 amending Decision No. 2014/512/CFSP concerning restrictive measures in view of Russia’s actions destabilising the situation in Ukraine.

⁴⁴ См. https://mid.ru/ru/press_service/journalist_help/repressions/.

⁴⁵ Reuters, “Russia blocks access to BBC and Voice of America websites”, 4 March 2022.

⁴⁶ Dan Cohen, “Ukraine’s propaganda war: international PR firms, DC lobbyists and CIA cutouts”, Mint Press News, 22 March 2022.

⁴⁷ Российское информационное агентство ТАСС, «Госдеп осудил решение суда РФ признать Facebook и Instagram экстремистскими организациями», 21 марта 2022 года, URL: <https://tass.ru/mezhdunarodnaya-panorama/14140065>.

частности, к 2010 году Европейский союз уже ввел ограничения на передачу программного обеспечения, особенно того, которое может иметь двойное (военное и гражданское) применение⁴⁸. Специальный докладчик признает, что правила Европейского союза предусматривают значительные списки исключений, включая программное обеспечение, являющееся общественным достоянием, которое конечные пользователи могут получить у розничных продавцов и установить без внешней поддержки⁴⁹.

26. Соединенные Штаты расширили список ограничений на торговлю программным обеспечением, включив в него «технологии и программное обеспечение, относящиеся к обработке материалов, электронике, телекоммуникациям, информационной безопасности, датчикам и лазерам, а также двигательным установкам», в том числе традиционное шифровальное и геопространственное программное обеспечение⁵⁰. В результате этого компании, разрабатывающие программное обеспечение под юрисдикцией Соединенных Штатов, обеспокоены необходимостью соблюдать санкционный режим в отношении торговли программным обеспечением, предоставляемым в рамках открытых для широкой публики предложений, которое используется в частных целях, а иногда даже бесплатно⁵¹, в ряд стран, включая (по состоянию на 2017 год) балканские страны, Беларусь, Демократическую Республику Конго, Зимбабве, Ирак, Иран (Исламская Республика), Корейскую Народно-Демократическую Республику, Кот-д'Ивуар, Кубу, Ливан, Ливию, Мьянму, Сирийскую Арабскую Республику⁵², Сомали и Судан, а также крайне обеспокоены растущим уровнем пиратства программного обеспечения.

27. Из-за запрета на экспорт технологий Сирийская Арабская Республика не смогла приобрести программное обеспечение, производимое только американскими компаниями, для компьютерных томографов и аппаратов искусственной вентиляции легких⁵³, используемых при лечении коронавирусного заболевания (COVID-19), а также для оказания других жизненно важных услуг⁵⁴. Зимбабве сообщила, что для получения доступа к необходимому программному обеспечению порой необходимо обращаться к посредникам или же платить гораздо более высокую цену, а в некоторых случаях доступа вообще не существует, поскольку поставщики отказываются продавать такое программное обеспечение Зимбабве или по причине потенциального перехвата платежей⁵⁵. Та же проблема касается и оборудования для государственных служб; Исламская Республика Иран

⁴⁸ Council of the European Union, document ST/5470/2020/INIT, pp. 1–37; Council of the European Union Regulation No. 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, art. 2 (1); Council of the European Union Regulation No. 267/2012 of 23 March 2012 concerning restrictive measures against Iran and repealing Regulation No. 961/2010, art. 2 (2); Council of the European Union Regulation No. 2016/44 of 18 January 2016 concerning restrictive measures in view of the situation in Libya and repealing Regulation No. 204/2011, annex I, para. 6; и Council of the European Union Regulation No. 401/2013 of 2 May 2013 concerning restrictive measures in respect of Myanmar/Burma and repealing Regulation No. 194/2008, art. 3 (b) and (c).

⁴⁹ Council of the European Union Regulation No. 428/2009 of 5 May 2009, annex I and Council of the European Union Regulation No. 401/2013 of 2 May 2013, annex III.

⁵⁰ Gibson Dunn, “2020 Mid-year sanctions and export controls update”, 4 August 2020.

⁵¹ Tyler Fuller, “Global software collaboration in the face of sanctions”, GitHub, 12 September 2019.

⁵² Материалы, представленные Сирийской Арабской Республикой.

⁵³ Нота 100/20 Постоянного представительства при Организации Объединенных Наций Сирийской Арабской Республики и материалы, представленные Зимбабве.

⁵⁴ Материалы, представленные Сирийской Арабской Республикой.

⁵⁵ Материалы, представленные Зимбабве.

сообщила о проблемах с приобретением программного обеспечения для медицинского оборудования и оборудования для мониторинга землетрясений⁵⁶.

28. Специальный докладчик подчеркивает, что с проблемами при закупке информационно-технического оборудования и программного обеспечения в странах, находящихся под санкциями, сталкиваются даже отделения самой Организации Объединенных Наций⁵⁷.

29. Кроме того, ей также известно о последствиях соблюдения и чрезмерного соблюдения санкций частным сектором. Как сообщается, из-за опасения вторичных санкций компании, находящиеся под юрисдикцией Соединенных Штатов, соблюдают ограничения, касающиеся программного обеспечения, традиционно используемого для обычного администрирования и общественных и частных целей, в частности, для оказания коммерческих услуг в Интернете или подключения к сети⁵⁸, и даже для некоммерческой деятельности.

30. В каждом конкретном случае Управление по контролю за иностранными активами Министерства финансов Соединенных Штатов решает, нарушает ли предложение конкретных услуг санкции Соединенных Штатов. Сообщается, что на сегодняшний день единственной технологической компанией, получившей лицензию на предоставление ранее ограниченных услуг для иранцев является «ГитХаб»; по словам представителей «ГитХаб», этот сложный процесс занял два года⁵⁹. Отсутствие ясности в отношении заявок, длительный и сложный процесс, а также потенциальные дополнительные расходы, вероятно, оттолкнул другие технологические платформы от попыток получить такие лицензии⁶⁰.

31. В этой связи Специальный докладчик с сожалением отмечает растущее число мер, препятствующих доступу граждан стран, находящихся под санкциями, к онлайн-платформам для ученых и специалистов (включая медицинских работников)⁶¹. Сообщается, что с июля 2020 года доступ иранских пользователей к своим услугам ограничили не менее 300 компаний⁶². Услуги видеоконференций, такие как «Зум»⁶³, большинство услуг «Гугл», а также образовательные ресурсы или услуги, связанные с работой в образовательной области, такие как «Юдеми»⁶⁴, облачный сервис «Амазон», «ГоуДэдди», «ГоуФандМи», «Академия «Хан»», «Курсера», «ГитЛаб», «Слак» и «ДиджиталОушен», иранцам больше не предоставляются⁶⁵. Сообщается, что некоторые международные облачные провайдеры, такие как «ДиджиталОушен», прекратили предоставлять хостинг

⁵⁶ Доклад о страновом визите в Исламскую Республику Иран (готовится к публикации).

⁵⁷ Конфиденциальные материалы.

⁵⁸ United States, Office of Foreign Assets Control, Executive Order No. 13685 of 19 December 2014 on blocking property of certain persons and prohibiting certain transactions with respect to the Crimea region of Ukraine: general license No. 9 on exportation of certain services and software incident to Internet-based communications authorized.

⁵⁹ Nat Friedman, "Advancing developer freedom: GitHub is fully available in Iran", GitHub, 5 January 2021.

⁶⁰ Center for Human Rights in Iran, "U.S. Government, companies can do more to promote Internet freedom in Iran", 17 March 2021.

⁶¹ Доклад Совету по правам человека.

⁶² Ali Borhani, "List of sites which block IPs come from Iran", GitHub, last updated 16 July 2020.

⁶³ Melody Kazemi, "Policy monitor – February 2021: alongside a localised internet shutdown in Sistan and Baluchestan, Iranian authorities unveiled several new proposals to regulate online speech", Filterwatch, 12 March 2021, URL: <https://filter.watch/en/2021/03/12/policy-monitor-february-2021>.

⁶⁴ Материалы, представленные от имени группы «Миаан».

⁶⁵ Материалы, представленные Исламской Республикой Иран.

представителям иранского частного сектора без предварительного уведомления, тем самым повысив их зависимость от других платформ и внутренних систем⁶⁶.

32. «Зум» и некоторые другие платформы были недоступны для жителей и граждан ряда стран, находящихся под санкциями, в том числе для учебных целей или даже для общения между врачами для обсуждения симптомов, диагностики и средств лечения, в том числе в отношении COVID-19. С 2020 года перечень ограничений в соглашении об обслуживании «Зум» существенно расширился⁶⁷. Это сделало невозможным использование «Зум» даже для связи с Организацией Объединенных Наций, как планировалось изначально. В частности, в 2020 году Куба не смогла принять участие в проводимой с помощью платформы «Зум» встрече на высшем уровне Организации государств Африки, Карибского бассейна и Тихого океана для обсуждения вопросов, касающихся пандемии COVID-19⁶⁸.

33. Специальный докладчик была проинформирована о том, что студенты, ученые и специалисты из стран, находящихся под санкциями, сталкиваются с проблемами в получении доступа к профессиональным базам данных. В частности, после того, как сервер медицинской базы данных «ПабМед» был передан компании «Гугл», иранские и сирийские врачи не смогли получить к ней доступ⁶⁹. Нередко они не могут зарегистрироваться в базах данных из-за отсутствия их стран гражданства в списках стран, в которых доступна эта услуга, или из-за отказа жителям и гражданам находящихся под санкциями стран. Это приводит к дискриминации, изоляции ученых и специалистов и невозможности получить доступ к знаниям (по сообщениям из Зимбабве⁷⁰, Ирана (Исламская Республика)⁷¹ и Сирийской Арабской Республики⁷²). Кроме того, имеются сложности с подпиской на онлайн-услуги, поскольку санкции препятствуют платежам.

34. Некоторые доклады также отражают растущее чрезмерное выполнение санкций платформами электронной торговли на основании подозрений в наличии какой-либо связи со странами, находящимися под санкциями. Так, по словам одного из пользователей, в 2020 году компания «Этси» удалила товар, обозначенный как «персидские куклы», выставленный на продажу на ее платформе, несмотря на то, что куклы были сделаны в Соединенных Штатах с использованием материалов из Соединенных Штатов.

35. Специальный докладчик также с озабоченностью отмечает, что, по сообщениям, из-за введения «санкционных оговорок» ученые из стран, против которых направлены санкции (Венесуэла (Боливарианская Республика), Иран (Исламская Республика), Российская Федерация и Сирийская Арабская Республика), лишены самой возможности представлять свои статьи для публикации, в

⁶⁶ Материалы, представленные от имени группы «Миаан» и материалы, представленные Сирийской Арабской Республикой.

⁶⁷ «Зум», «Условия обслуживания Zoom», 13 апреля 2022 года, URL: <https://explore.zoom.us/ru/terms/>.

⁶⁸ Granma, “Bloqueo de EE.UU. impide a Cuba participar en foro multilateral; capturados en Venezuela 57 mercenarios; protestas por racismo en EE.UU.; Bolsonaro bloquea fondos para lucha contra la COVID-19”, 5 June 2020, URL: www.granma.cu/hilo-directo/2020-06-05/hilo-05-06-2020-00-06-14.

⁶⁹ Ответы и комментарии Исламской Республики Иран.

⁷⁰ Доклад о страновом визите в Исламскую Республику Иран (готовится к публикации).

⁷¹ Материалы, представленные Сирийской Арабской Республикой.

⁷² Материалы, представленные Зимбабве.

том числе в онлайн-журналах, из-за своего гражданства⁷³, ⁷⁴. Это приводит к изоляции людей, занимающихся искусством, наукой и спортом⁷⁵.

36. Она также отмечает расширяющуюся практику среди провайдеров онлайн-услуг закрывать учетные записи, блоги и каналы внесенных и не внесенных в санкционные перечни лиц и компаний. Блокировка аккаунтов в социальных сетях осуществляется, в частности, компаниями, зарегистрированными в Соединенных Штатах в рамках режима санкций, введенного в соответствии с законом Магнитского⁷⁶.

37. Также сообщалось, что в 2021 году ряд каналов и аккаунтов «Ютуб», принадлежащих белорусским средствам массовой информации, были заблокированы, а журналисты были внесены в санкционные перечни⁷⁷. «Твиттер», «Ютуб», «Спотифай», «ТикТок» и «Мета» заблокировали аккаунты, принадлежащие средствам массовой информации Российской Федерации, которые считаются связанными с государством. «Гугл» и «Инстаграм» понизили ссылки на средства массовой информации Российской Федерации в результатах поиска, что сократило доступ к этим средствам массовой информации на 90 процентов⁷⁸. «Мета» ввела ограничения в связи с распространением фальшивых новостей из Российской Федерации и Беларуси с использованием поддельных аккаунтов в социальных сетях⁷⁹.

IV. Другие аспекты применения санкций в цифровой сфере

38. Специальный докладчик также подчеркивает, что доступ к Интернету и информации может быть предотвращен санкциями косвенным образом. Нехватка топлива в Боливарианской Республике Венесуэла приводит к отключению электричества, что довольно часто делает доступ к Интернету невозможным, а снижение доходов делает доступ к Интернету невозможным для большинства жителей Венесуэлы (Боливарианской Республики)⁸⁰, Зимбабве, Сирийской Арабской Республики и многих других стран⁸¹.

39. Недоступность необходимого оборудования, запасных частей и программного обеспечения, а также финансовых операций с ними приводит к сокращению зон покрытия интернет-коммуникаций. В частности, охват Интернетом в Боливарианской Республике Венесуэла снизился с 50–90-процентного охвата в 2015 году, до введения санкций, до 10-процентного охвата⁸². В Сирийской

⁷³ Доклад о страновом визите в Исламскую Республику Иран (готовится к публикации) и Office of the United Nations High Commissioner for Human Rights, “Unilateral sanctions threaten scientific research and academic freedom: UN experts”, 7 July 2022.

⁷⁴ Communications USA 9/2022; ОН 37/2022; ОН 38/2022; ОН 39/2022; и ОН 40/2022, URL: <https://spcommreports.ohchr.org/TmSearch/Mandates?m=263>.

⁷⁵ Материалы, представленные Сирийской Арабской Республикой.

⁷⁶ Donie O’Sullivan and Artemis Moshtaghian, “Instagram says it’s removing posts supporting Soleimani to comply with US sanctions”, CNN Business, 13 January 2020, URL: <https://edition.cnn.com/2020/01/10/tech/instagram-iran-soleimani-posts/index.html> и Jonny Tickle, “Chechen leader Kadyrov banned from Instagram again, loses account with 1.4 million followers”, RT, 13 May 2020, URL: www.rt.com/russia/488533-kadyrov-banned-instagram-again/.

⁷⁷ Материалы, представленные Беларусью.

⁷⁸ См. https://mid.ru/ru/press_service/journalist_help/repressions/.

⁷⁹ Sergiu Gatlan, “Meta: Ukrainian officials, military targeted by Ghostwriter hackers”, Bleeping Computer, 28 February 2022.

⁸⁰ A/HRC/48/59/Add.2.

⁸¹ Материалы, представленные организацией «Безотлагательный доступ».

⁸² A/HRC/48/59/Add.2.

Арабской Республике охват услугами фиксированной связи сократился на 38 процентов, охват мобильным Интернетом — на 15 процентов, а охват Интернетом — на 7 процентов⁸³.

40. Специальный докладчик также обеспокоена угрозами и публичными обвинениями в Интернете в том, что отдельные лица или компании, как внесенные в санкционные перечни, так и не внесенные, занимаются преступной деятельностью. Она обращает особое внимание на предложения о вознаграждении, сделанные Соединенными Штатами на официальном сайте «Вознаграждение за помощь правосудию» и в Твиттере за обнаружение лиц, предположительно причастных к террористической деятельности, без возбуждения против них каких-либо судебных дел⁸⁴.

41. Довольно часто страны, столкнувшиеся с серьезными экономическими санкциями, разрабатывают собственную криптовалюту (например, Венесуэла (Боливарианская Республика) и Корейская Народно-Демократическая Республика). Соединенные Штаты теперь вводят санкции за использование этих криптовалют в транзакциях⁸⁵.

V. Правовая оценка использования односторонних санкций в киберпространстве и их гуманитарного воздействия

42. Специальный докладчик сожалеет, что правовая оценка применения санкций и других видов принудительных мер в ответ на злонамеренную деятельность как правило не проводится и что понятие «злонамеренность» не имеет единого определения.

43. Международный комитет Красного Креста (МККК) утверждает, что для того, чтобы квалифицировать использование кибертехнологий как вооруженное нападение, оно должно ставить под угрозу само существование государства⁸⁶; приводить к потере человеческих жизней (гибели или ранению комбатантов или гражданских лиц), уничтожению или повреждению имущества (гражданского или военного), включая объекты критически важной инфраструктуры⁸⁷, или потере части территории государства⁸⁸; иметь причинно-следственную связь с непосредственными негативными последствиями (с промежутком в секунды

⁸³ Материалы, представленные Сирийской Арабской Республикой.

⁸⁴ См. сообщение USA 9/2021, URL: <https://spcommreports.ohchr.org/TMResultsBase/DownloadPublicCommunicationFile?gId=25985>.

⁸⁵ Alexander Galicki, “U.S. sanctions Venezuela’s “Petro” cryptocurrency amid broader trend of sanctioned and rogue regimes experimenting with digital assets”, Clearly Gottlieb, 13 April 2018.

⁸⁶ Yoram Dinstein, *War, Aggression and Self-Defence* (Cambridge University Press, 2001), pp. 175–176; Jochen A. Frowein, “Legal consequences for international law enforcement in case of Security Council inaction”, in *The Future of International Law Enforcement: New Scenarios, New Law?*, Jost Delbrück, ed., (Berlin, Dunker and Humblot, 1993).

⁸⁷ Michael Schmitt, “‘Attack’ as a term of art in international law: the cyber operations context”, in *Proceedings of the 4th International Conference on Cyber Conflict*, Christian Czosseck, Rain Ottis and Katharina Ziolkowski, eds., (2012), pp. 287–288 and Marco Roscini, “World wide warfare — ‘jus ad bellum’ and the use of cyber force”, in *Max Planck Yearbook of United Nations Law*, Armin von Bogdandy and Rüdiger Wolfrum, eds., vol. 14 (Brill, 2010), pp. 106–107.

⁸⁸ Pauline C. Reich and others, “Cyber warfare: a review of theories, law, policies, actual incidents — and the dilemma of anonymity”, *European Journal of Law and Technology*, vol. 1, No. 2 (2010).

или минуты между нападением и его результатами)⁸⁹; и быть приписываемым конкретному государству в соответствии с правом международной ответственности. Специальный докладчик подчеркивает, что в соответствии со статьей 51 Устава Организации Объединенных Наций только нападения, отвечающие вышеуказанным критериям, могут служить основанием для актов самообороны.

44. Она также подчеркивает, что «нападение на объекты критически важной инфраструктуры» может пониматься по-разному и может быть интерпретировано как нападения на плотины, атомные электростанции, системы контроля над вооружениями, банковские счета и операции, газо- и нефтепроводы, линии электропередачи, системы налогообложения, правительственные серверы и компьютерные сети⁹⁰ и другие объекты критически важной инфраструктуры, а также перехват контроля над системами противовоздушной обороны⁹¹, шлюзами плотин, самолетами или поездами (что может привести к их столкновению)⁹². В частности, Исламская Республика Иран ссылается на атаку 2021 года, которая остановила работу более чем 4300 автозаправочных станций (примерно 70 процентов всех автозаправочных станций в стране), в результате чего десятки миллионов иранцев не могли получить доступ к топливу. Исламская Республика Иран также ссылается на произошедшую в 2010 году атаку «Стакснет», которая была осуществлена враждебным поставщиком через платформу центрифуги в ядерном реакторе в Нетензе⁹³.

45. Специальный докладчик хотела бы подчеркнуть, что режим борьбы с международным терроризмом в киберпространстве определен в резолюциях Совета Безопасности, которые обязывают государства принимать широкий спектр мер по предотвращению использования кибертехнологий для распространения враждебной пропаганды, подстрекательства к насилию, отмывания денег и финансирования терроризма, оправдания террористической деятельности и идеологии, участия в террористической деятельности, планирования и совершения террористических актов⁹⁴.

46. Она подчеркивает, что меры по выполнению резолюций Совета Безопасности, включая внесение в санкционные перечни конкретных лиц и компаний за злонамеренную активность с использованием киберсредств, могут осуществляться только в полном соответствии с предоставленными полномочиями, и что

⁸⁹ ICRC, Commentary of 2016 on article 2 of the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, para. 255 and Heather Harrison Dinness, *Cyber Warfare and the Laws of War* (Cambridge University Press, 2014), pp. 63–73.

⁹⁰ Reich and others, “Cyber warfare”, pp. 12–17.

⁹¹ International Law Association, “Draft report on aggression and the use of force”, May 2016, p. 18, URL: <https://ila.vettoreweb.com/Storage/Download.aspx?DbStorageId=1055&StorageFileGuid=c911005c-6d63-408e-bc2d-e99bfc2167e4>.

⁹² МККК, Комментарий от 2016 года к статье 3 Женевской конвенции об улучшении участи раненых и больных в действующих армиях, п. 437.

⁹³ Материалы, представленные Исламской Республикой Иран.

⁹⁴ Резолюция Совета Безопасности 2462 (2019), преамбула и пункты 19 и 20, и резолюция Совета Безопасности 2419 (2018), преамбула.

введение дополнительных односторонних санкций⁹⁵ или других принудительных мер при несоблюдении решений Совета Безопасности⁹⁶ не имеет оснований в международном праве.

47. Таким образом, Специальный докладчик хотела бы отметить, что государства могут принимать односторонние меры в ответ на злонамеренную киберактивность только в том случае, если они не нарушают никаких международных обязательств, в том числе в сфере прав человека (реторсии), или если их противоположность исключается в соответствии с международным правом в ходе принятия контрмер⁹⁷.

48. Контрмеры могут быть приняты потерпевшими государствами только в ответ на нарушение конкретного международного обязательства конкретным государством и могут быть направлены только против этого государства⁹⁸ с целью побудить его к соблюдению обязательства в соответствии с принципами необходимости и соразмерности нарушению и запретами на нарушение императивных норм международного права, применение силы, несанкционированные репрессии или нарушение основных прав человека⁹⁹. Чтобы законно принять контрмеры, государство должно быть в состоянии доказать наличие у предполагаемого преступника «реального»¹⁰⁰ или «общего»¹⁰¹ контроля над злонамеренным киберактом.

49. В этом отношении Специальный докладчик согласна с позицией, занятой составителями Таллиннского руководства 2.0, а именно: к деятельности в киберсфере должны применяться те же правила присвоения деятельности негосударственных субъектов государствам (действующим под их руководством и контролем), поскольку международное право не предусматривает никакого

⁹⁵ Vera Gowlland-Debbas, "The limits of unilateral enforcement of community objectives in the framework of UN peace maintenance", *European Journal of International Law*, vol. 11 (2000); Peter Malanczuk, *Humanitarian Intervention and the Legitimacy of the Use of Force* (The Hague, Het Spinhuis 1993), pp. 17–19; Rein Müllerson, "Jus ad bellum and international terrorism" in *International Law and the War on Terror*, Fred L. Borch and Paul S. Wilson, eds., (Newport, Rhode Island, Naval War College, 2003), p. 175; Michael Byers, "Terrorism, the use of force and international law after 11 September", *International and Comparative Law Quarterly*, vol. 51 (2002), p. 401; Alexander Orakhelashvili, "The impact of peremptory norms on the interpretation and application of United Nations Security Council resolutions", *European Journal of International Law*, vol. 16 (2005); and Hartmut Körbs, *Die Friedenssicherung durch die Vereinten Nationen und Regionalorganisationen* (Bochum, Brockmeyer, 1997), p. 538.

⁹⁶ Rainer Hofmann, "International law and the use of military force against Iraq", *German Yearbook of International Law*, vol. 45 (2002); Edward McWhinney, "International law-based responses to the September 11 international terrorist attacks", *Chinese Journal of International Law*, vol. 1 (2002), p. 282; и Christian Schaller, "Massenvernichtungswaffen und präventivkrieg — möglichkeiten der rechtverfolgung einer militärischen intervention im Irak aus völkerrechtlicher sicht", *German Yearbook of International Law*, vol. 62 (2002), p. 654.

⁹⁷ См. Alena F. Douhan, *Regional Mechanisms of Collective Security: The New Face of Chapter VIII of the UN Charter?* (Paris, L'Harmattan, 2013), pp. 98–112.

⁹⁸ See Dorothee Geyrhalter, *Friedenssicherung durch Regionalorganisationen ohne Beschluß des Sicherheitsrates* (Cologne, LIT, 2001), p. 66.

⁹⁹ Статьи об ответственности государств за международно-противоправные деяния, ст. 48 51. Дороти Гейрхальтер, например, утверждает, что возможно применение экономических санкций против государств, ответственных за массовые нарушения основных прав человека; см. Geyrhalter, *Friedenssicherung durch Regionalorganisationen ohne Beschluß des Sicherheitsrates*, p. 66. См. также Antonios Tzanakopoulos, "State responsibility for 'targeted sanctions'", *American Journal of International Law*, vol. 113 (2019), pp. 136–137.

¹⁰⁰ Международный суд, Дело о военной и военизированной деятельности в Никарагуа и против Никарагуа (Никарагуа против Соединенных Штатов Америки) решение от 27 июня 1986 года, пункты 113–115.

¹⁰¹ International Tribunal for the Former Yugoslavia, Appeals Chamber, *The Prosecutor v. Duško Tadić*, Case no. IT-94–1–A, 15 July 1999, paras. 120–124 and 146.

дополнительного или иного регулирования¹⁰². Таким образом, контрмеры не могут также применяться к физическим или юридическим лицам, обвиняемым в совершении киберпреступлений¹⁰³.

50. Специальный докладчик хотела бы отметить, что использование односторонних санкций против государственных органов и должностных лиц не соответствует принципу суверенного равенства государств или положениям об иммунитете государств и их собственности, особенно когда санкции приводят к аресту имущества компаний, контролируемых государством. Она подчеркивает, что иммунитет государств и их собственности является абсолютным. Поскольку административное решение предоставляет еще меньше гарантий, чем судебный процесс, отказ в предоставлении иммунитета на основании такого решения нарушает международное право.

51. В этой связи положение, содержащееся в пункте 6 статьи 1 Регламента Совета Европейского союза № 2019/796 от 2019 года, не соответствует требованию, изложенному в пункте 1 статьи 49 статей об ответственности государств за международно-противоправные деяния, поскольку в нем говорится о введении санкций в тех случаях, «когда это считается необходимым для достижения общих целей внешней политики и политики безопасности», а не в ответ на международно-противоправное деяние. Более того, положение, позволяющее применять ограничительные меры «в ответ на кибератаки, имеющие значительное воздействие на третьи государства или международные организации», а не на Европейский Союз или его государства-члены, не относится к якобы нарушенным обязательствам, имеющим характер *erga omnes*, и противоречит статье 48 статей об ответственности государств за международно-противоправные деяния.

52. Некоторые специалисты по публичному праву отмечают, что соответствующее постановление Европейского союза направлено на предоставление ему финансовых рычагов для прямого, более жесткого и эффективного наказания за кибератаки¹⁰⁴. Отмечается, что государства, применяющие санкции, предпочитают этот подход уголовному преследованию. На практике требования о бремени доказывания и надлежащей правовой процедуры в отношении кибератак соблюсти нелегко¹⁰⁵, но Специальный докладчик подчеркивает, что санкции не могут быть карательными¹⁰⁶ и должны соответствовать международным правовым стандартам.

53. Специальный докладчик также обеспокоена тем, что даже когда односторонние санкции вводятся против отдельных лиц и компаний за действия в киберпространстве и нет доказательств их приписывания конкретному государству, они все равно представляются как санкции против государств (как, например, в законе «О противодействии российскому влиянию в Европе и Евразии» и законе «О противодействии противникам Америки посредством санкций», принятых Соединенными Штатами)¹⁰⁷.

¹⁰² Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed., (Cambridge University Press, 2017), pp. 94–96.

¹⁰³ Ibid., pp. 111–122.

¹⁰⁴ Ali Abusedra, Abu Bakar Munir and Md Toriqul Islam, “Use of cyber means to enforce unilateral coercive measures in international law”, in *Unilateral Sanctions in International Law*, Surya P. Subedi, ed. (Oxford, Hart Publishing, 2021), p. 317.

¹⁰⁵ Ibid., p. 320.

¹⁰⁶ Alexander Kern, *Economic Sanctions: Law and Public Policy* (New York, Palgrave Macmillan, 2009).

¹⁰⁷ См. также Office of Foreign Assets Control, “North Korea Sanctions Program”, updated 2 November 2016, p. 5, URL: <https://home.treasury.gov/system/files/126/nkorea.pdf>.

54. Признавая, что государства несут обязательства по принятию мер по пресечению киберпреступлений против государства, его граждан и юридических лиц, такие меры должны оставаться в признанных международных рамках: присоединение к международным договорам, разработка законодательства, начало уголовного расследования и преследования и сотрудничество в судебной сфере¹⁰⁸. Специальный докладчик подчеркивает, что такие меры должны приниматься только при условии полного соблюдения международных и национальных стандартов в области прав человека.

55. Однако современная практика показывает, что люди вносятся в списки в связи с совершением киберпреступлений против государства, граждан государства или его юридических лиц исполнительными, а не судебными органами, что лишает их доступа к правосудию и права на надлежащее судебное разбирательство. Согласно данным, полученным из конфиденциальных источников, решения принимаются на основе секретной информации и не разглашаются. Более того, даже возможность обжаловать включение в санкционный список Соединенных Штатов очень ограничена, а сам процесс длителен и недешев. В результате человек теряет возможность защищать свои права в суде, и тем самым нарушаются его имущественные права, свобода передвижения, право на защиту личной жизни и право на репутацию, а также экономические, трудовые и социальные права.

56. В этом отношении примечательна недавняя практика Соединенных Штатов. В 2020 году в список Управления по контролю за иностранными активами были включены шесть нигерийцев за кражу более 6 миллионов долларов у жертв по всей территории Соединенных Штатов посредством мошенничества с использованием схем в киберпространстве¹⁰⁹. Пресс-релиз содержит информацию о предполагаемой деятельности каждого из этих лиц, их фотографии и другие личные данные, а также предполагаемые мошеннические схемы так, словно это — подтвержденные факты. В 2020 году такой же подход был применен к двум российским гражданам.

57. В этой связи неясно, почему в связи с предполагаемыми киберпреступлениями не было возбуждено уголовное дело. Вместо этого были приняты меры в виде односторонних санкций по решению исполнительного органа, Управления по контролю за иностранными активами, без какого-либо упоминания о возбуждении уголовного дела или какой-либо возможности для перечисленных лиц получить доступ к судам для защиты своих прав, репутации или персональных данных.

58. Более того, введение экономических санкций и запретов на въезд, помимо нарушения прав собственности и других прав, также противоречит требованию презумпции невиновности, изложенному в пункте 2 статьи 14 Международного пакта о гражданских и политических правах, которое рассматривается Комитетом по правам человека как гарантия, которую «государства-участники обязаны соблюдать, независимо от их юридических традиций и внутреннего права»¹¹⁰. В пункте 30 своего замечания общего порядка № 32 (2007) о праве на равенство перед судами и трибуналами и на справедливое судебное разбирательство

¹⁰⁸ Решение ОБСЕ № 7/06 от 5 декабря 2006 года и OSCE, “Executive summary of regional workshop on countering the use of the Internet for terrorist purposes for judges, prosecutors and investigators from South Eastern Europe”.

¹⁰⁹ United States, Department of the Treasury, “Treasury sanctions Nigerian cyber actors for targeting U.S. businesses and individuals”, press releases of 16 June 2020, URL: <https://home.treasury.gov/news/press-releases/sm1034>.

¹¹⁰ Замечание общего порядка Комитета по правам человека № 32 (2007) о праве на равенство перед судами и трибуналами и на справедливое судебное разбирательство, п. 4.

Комитет прямо отмечает, что презумпция невиновности гарантирует, что «никакая вина не может быть презюмирована до тех пор, пока виновность не была доказана вне всяких разумных сомнений», и «обеспечивает, чтобы сомнения толковались в пользу обвиняемого»; кроме того, Комитет просит правительства воздерживаться от публичных заявлений, в которых утверждается о виновности обвиняемого. В своем замечании общего порядка № 16 (1988) о праве на личную жизнь Комитет ссылается на обязательство государств не только не посягать на честь и репутацию отдельных лиц, но и обеспечить надлежащее законодательство, гарантирующее их защиту¹¹¹. Специальный докладчик с озабоченностью отмечает, что при введении санкций в отношении киберпреступлений ни одно из вышеперечисленных требований не соблюдается.

59. В результате широкое распространение негативной информации о физических и юридических лицах в обход презумпции невиновности и гарантий надлежащей правовой процедуры снижает, в частности, их привлекательность для инвесторов и контрагентов, что приводит к чрезмерному соблюдению санкционных режимов.

60. Статья 275 Договора о функционировании Европейского Союза предусматривает возможность обжалования наложения санкций в Суде Европейского Союза¹¹², однако Суд обычно фокусируется на оценке предоставления минимальных процессуальных гарантий и избегает вопроса о правах собственности как подлежащих ограничению при определенных условиях¹¹³, а также вопросов презумпции невиновности и репутационных рисков. На сегодняшний день не было сделано никаких заявлений о пересмотре санкций, введенных в связи со злонамеренными действиями в информационном пространстве.

61. Специальный докладчик отмечает, что обещание вознаграждения, предлагаемого на веб-сайте и в Твиттере программы «Вознаграждение за помощь правосудию» Соединенных Штатов за обнаружение лиц, предположительно причастных к террористической деятельности, без возбуждения против них какого-либо дела и довольно часто без надлежащей проверки информации¹¹⁴, не только разрушает их репутацию, но и может поставить под угрозу их жизнь.

62. Специальный докладчик подчеркивает, что обязательство государств гарантировать равное участие в академическом сотрудничестве и доступ к информации, а также право пользоваться плодами научного прогресса отражено Комитетом по экономическим, социальным и культурным правам в его замечании общего порядка № 25 (2020) о науке и экономических, социальных и культурных правах¹¹⁵. Таким образом, лишение граждан или жителей конкретной страны доступа к профессиональным базам данных или платформам, возможности использовать эти платформы для преподавания или общения, а также подавать рукописи для публикации по причине их гражданства или места проживания представляет собой дискриминацию по признаку гражданства или места проживания и приводит к нарушению прав на доступ к информации и свободу коммуникации и академических свобод. Представители Венесуэлы (Боливарианская Республика), Ирана (Исламская Республика) и Судана также сообщают о нарушениях

¹¹¹ Комитет по правам человека, замечание общего порядка № 16 (1988) о праве на личную жизнь.

¹¹² Treaty on the Functioning of the European Union, *Official Journal of the European Union*, 2012/C 326/01, pp. 47–390.

¹¹³ Bogdanova and Callo-Müller, “Unilateral cyber sanctions”, p. 938.

¹¹⁴ См. сообщение USA 9/2021, URL: <https://spcommreports.ohchr.org/TMResultsBase/DownloadPublicCommunicationFile?gId=25985>.

¹¹⁵ Комитет по экономическим, социальным и культурным правам, замечание общего порядка № 36 (2020) о науке и экономических, социальных и культурных правах, пп. 21 и 52.

права на образование в связи с невозможностью использовать онлайн-платформы в образовательных целях.

63. Специальный докладчик подчеркивает, что доступ к интернет-технологиям и интернет-ресурсам упоминается как неотъемлемый элемент не только борьбы с пандемией, но и права на развитие¹¹⁶. Такого же подхода придерживается Совет по правам человека¹¹⁷ и Специальный докладчик по вопросу о поощрении и защите права на свободу мнений и их выражения¹¹⁸. В своей Декларации о свободе обмена информацией в интернете Комитет министров Совета Европы призвал государства-члены «содействовать доступу для всех к коммуникационным и информационным услугам Интернета на недискриминационной основе по доступной цене и поощрять такой доступ» (принцип 4)¹¹⁹.

64. Декларация принципов «Построение информационного общества — глобальная задача в новом тысячелетии» призывает государства обеспечить доступ к информационно-коммуникационной инфраструктуре и технологиям, информации и знаниям для всех¹²⁰ и рассматривает информационно-коммуникационные технологии как средство содействия достижению целей в области развития, сформулированные в Декларации тысячелетия¹²¹.

65. В 2020 году Специальный докладчик по вопросу о современных формах расизма, расовой дискриминации, ксенофобии и связанной с ними нетерпимости верно отметила в своем докладе Совету по правам человека, что из-за бедности и неразвитости цифровой инфраструктуры люди из наименее развитых стран имеют лишь четверть возможности получить доступ к Интернету по сравнению с жителями других стран, что приводит к ограничению их доступа к информации о здоровье населения в Интернете и их готовности использовать цифровые платформы для обучения, работы и покупок, что особенно важно во времена COVID-19¹²².

66. Если речь идет о публично предлагаемых платных или бесплатных кибер-программах или услугах, то не следует говорить о возможности выбора торговых партнеров. Лишение людей в затронутых санкциями странах доступа к этим услугам нарушает ряд прав человека, включая права на доступ к информации, свободу общения, образование и достойную работу и другие экономические права, и представляет собой фактическую дискриминацию затронутых групп населения, составляющих около 20 процентов населения мира.

67. Еще одной правовой и правозащитной проблемой мандатария является возможность введения ограничений на вещание средств массовой информации в интернет-пространстве. Совет Безопасности неоднократно отмечал, что распространение информации может носить и злонамеренный характер, разжигать ненависть, вспышки экстремизма и радикализации населения и представлять угрозу для поддержания международного мира и безопасности¹²³, а

¹¹⁶ Социальный форум, состоявшийся 8 октября 2020 года.

¹¹⁷ Резолюция 32/13 Совета по правам человека, преамбула.

¹¹⁸ A/66/290, пп. 45–75.

¹¹⁹ Декларация, принятая Комитетом министров Совета Европы 28 мая 2003 года, URL: www.osce.org/fom/31507?download=true.

¹²⁰ Декларация, принятая 12 декабря 2003 года на пятом пленарном заседании женевского этапа Всемирной встречи на высшем уровне по вопросам информационного общества, пункты 19–28, URL: www.itu.int/net/wsis/docs/Geneva/official/dop.html.

¹²¹ Там же, пп. 1 и 2.

¹²² A/HRC/44/57, п. 20.

¹²³ Резолюция Совета Безопасности 2462 (2019), пункты 19 и 21, и Kalliopi Chainoglou, “Psychological warfare”, in *Max Planck Encyclopedias of International Law*, para. 3.

распространение враждебной пропаганды может нарушать положения статей 19 и 20 Международного пакта о гражданских и политических правах.

68. В своем замечании общего порядка № 36 (2018) о праве на жизнь Комитет по правам человека прямо заявляет, что распространение враждебной пропаганды и подстрекательство к военным действиям представляют собой прямое нарушение права на жизнь.

69. Совет по правам человека подчеркивает важность свободного, справедливого и сбалансированного доступа к информации для обеспечения права на развитие¹²⁴. Возможные ограничения предусмотрены в ряде международных договоров, включая Международный пакт о гражданских и политических правах в его статье 19, пункт 3 и статье 20, в том числе: а) пропаганда войны; б) высказывания в пользу национальной, расовой или религиозной ненависти, представляющие собой подстрекательство к дискриминации, вражде или насилию¹²⁵; с) приказы не оставлять никого в живых¹²⁶; d) прямое и публичное подстрекательство к совершению актов геноцида¹²⁷; e) распространение детской порнографии¹²⁸; f) распространение расистских и ксенофобских материалов с помощью онлайн средств, угроз и оскорблений¹²⁹; g) отрицание, крайняя минимизация, одобрение или оправдание геноцида или преступлений против человечности¹³⁰; и h) призывы к свержению правительства или участию в террористической деятельности¹³¹.

70. Специальный докладчик по вопросу о поощрении и защите права на свободу мнений и их свободное выражение неоднократно настаивала на том, что бремя доказывания обоснованности ограничений лежит на государстве¹³². В то же время ограничения должны толковаться как можно более узко, во избежание злоупотреблений¹³³.

71. В соответствии с пунктом 3 статьи 19 Международного пакта о гражданских и политических правах также возможно введение ограничений для уважения прав и репутации других лиц или для охраны государственной безопасности и общественного порядка, охраны здоровья или защиты нравственности населения. Аналогичный подход отражен в статье 34 Устава Международного союза электросвязи. В то же время любые ограничения должны вводиться исключительно на основании закона, в соответствии с замечанием общего порядка № 34 (2011) Комитета по правам человека о свободе мнений и их выражения, с уделением приоритетного внимания надлежащему соблюдению свободы выражения мнений¹³⁴.

72. Документы Европейского союза, санкционирующие введение ограничений на вещание «РТ» и «Спутника» в Евросоюзе, содержат ссылку на нарушение безопасности и общественного порядка и приверженность свободе выражения

¹²⁴ См. резолюцию 33/3 Совета по правам человека, п. 6 j).

¹²⁵ Международный пакт о гражданских и политических правах, ст. 20.

¹²⁶ Дополнительный Протокол к Женевским конвенциям от 12 августа 1949 года, касающийся защиты жертв международных вооруженных конфликтов, ст. 40.

¹²⁷ Конвенция о предупреждении преступления геноцида и наказании за него, ст. 3.

¹²⁸ Конвенция Совета Европы о киберпреступности, ст. 9.

¹²⁹ Дополнительный протокол к Конвенции о киберпреступности, касающийся уголовной ответственности за акты расистского и ксенофобского характера, совершаемые через компьютерные системы, ст. 3–5.

¹³⁰ Там же, ст. 6.

¹³¹ de Brabandere, “Propaganda”.

¹³² A/HRC/29/32, пп. 32–35 и A/67/357, пп. 41 и 45.

¹³³ A/66/290, п. 24 и A/67/357, п. 45.

¹³⁴ A/66/290, пункты 24–30 и 46.

мнения и вводятся на основании закона¹³⁵. В то же время в этих положениях не отражен ни один из критериев, разработанных Комитетом по правам человека в его общих комментариях. Обоснование для принятия правил не было объявлено каким-либо другим способом. Попытка «РТ Франс» оспорить введение запрета на вещание и потребовать его отмены в качестве временной меры оказалась безрезультатной в Суде Европейского союза, который постановил об отсутствии доказательств наличия гуманитарного и социального вреда, обязанность доказывания которого лежит на «РТ Франс»¹³⁶.

73. Специальный докладчик также отмечает существующие проблемы с оценкой законности полномочий операторов онлайн-платформ и их обязательств по международному праву, особенно обязательства по защите прав человека¹³⁷. Как и другие предприятия, они должны избегать ущемления прав человека других лиц и устранять неблагоприятное воздействие на права человека, к которому они причастны, и стремиться предотвратить или смягчить неблагоприятное воздействие на права человека, которое непосредственно связано с их деятельностью, продукцией, услугами или деловыми отношениями, в соответствии с Руководящими принципами предпринимательской деятельности в аспекте прав человека (принципы 11–13).

74. Именно по этой причине Специальный докладчик предостерегает государства от использования социальных сетей и средств массовой информации для ведения пропаганды, распространения непроверенной информации или призывов к насилию. Например, разрешение социальной сети «Фейсбук» компании «Мета» на размещение материалов, призывающих к насилию в отношении российских граждан и должностных лиц¹³⁸ в связи с развитием кризиса 2022 года на Украине¹³⁹, позднее пересмотренное¹⁴⁰, нарушило статьи 19 и 20 Международного пакта о гражданских и политических правах и привело к всплеску русофобии во многих странах; оно было осуждено Верховным комиссаром по правам человека и Генеральным секретарем¹⁴¹.

¹³⁵ Постановление Совета Европейского Союза № 2022/350, пункт 8.

¹³⁶ Court of Justice of the European Union, “Opération militaire en Ukraine: le président du Tribunal rejette la demande de RT France visant à suspendre les sanctions adoptées par le Conseil”, press release No. 54/22, Order of the President of the General Court in case T-125/22, 30 March 2022, URL: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-03/cp220054fr.pdf>.

¹³⁷ Enguerrand Marique and Yseult Marique, “Sanctions on digital platforms: balancing proportionality in a modern public square”, *Computer Law and Security Review*, October 2019, pp. 4–5.

¹³⁸ Munsif Vengattil and Elizabeth Culliford, “Facebook allows war posts urging violence against Russian invaders”, Reuters, 11 March 2022.

¹³⁹ Mark Trevelyan, “Facebook owner defends policy on calls for violence that angered Russia”, Reuters, 14 March 2022.

¹⁴⁰ Katie Paul and Munsif Vegattil, “How Meta fumbled propaganda moderation during Russia’s invasion of Ukraine”, Reuters, 11 April 2022.

¹⁴¹ Oops Top, “UN High Commissioner for Human Rights Bachelet speaks out against Russophobia”, 20 March 2022, URL: <https://oopstop.com/un-high-commissioner-for-human-rights-bachelet-speaks-out-against-russophobia/> и Aanchal Nigam, “UN condemns Facebook owner Meta for allowing ‘hate speech’ against Russians”, Republic World, 12 March 2022.

VI. Выводы и рекомендации

Выводы

75. Цифровые технологии меняют все аспекты человеческой жизни и международного права, включая сферу применения, субъекты, средства и методы международных и односторонних санкций. Одни санкции используются, в частности, в качестве ответных мер на киберсредства финансирования терроризма и злонамеренную активность с использованием киберсредств, включая атаки на критически важную инфраструктуру, не достигающие уровня вооруженного нападения, а другие направлены на киберпространство, в частности, путем предотвращения доступа к публичным онлайн-платформам, блокирования торговли программным обеспечением или информационно-коммуникационным оборудованием, блокирования аккаунтов в социальных сетях и включения криптовалют в перечень.
76. Это вызывает многочисленные проблемы в международном праве, включая право международной ответственности, право международной безопасности, международное гуманитарное право, право государственных иммунитетов, право международной торговли, право прав человека и международное частное право.
77. Некоторые односторонние санкции в киберсфере — предотвращение доступа к спутникам, Интернету, программному обеспечению, общедоступным информационно-коммуникационным платформам и услугам — затрагивают все население стран, ставших объектами санкций, и негативно влияют на их экономические и культурные права, включая права на Интернет, информацию, образование, здоровье, жизнь и развитие, а также академические свободы, и представляют собой дискриминацию по национальному признаку.
78. Деятельность физических и юридических лиц в киберпространстве может поставить под угрозу существование государств и может представлять угрозу международному миру и безопасности. Устав Организации Объединенных Наций не препятствует Совету Безопасности принимать решение о принятии принудительных мер в таких условиях. Сегодня выполнение решений Совета Безопасности включает в себя меры, принимаемые государствами в киберсфере.
79. Односторонние меры могут приниматься государствами и региональными организациями в ответ на злонамеренную активность с использованием киберсредств или использование киберсредств только в полном соответствии с международным правом, и только если эти меры также не нарушают никаких обязательств в сфере прав человека или гуманитарного права, или являются частью контрмер.
80. Целевые санкции как замена уголовного процесса в случаях киберпреступлений нарушают экономические права, право на свободу передвижения и право на надлежащую правовую процедуру. Публикация в Интернете списков лиц, в отношении которых применяются санкции, с предложением денежного вознаграждения и утверждением, что эти лица совершили преступления, без проведения расследований или вынесения судебных вердиктов, отрицательно сказывается на их репутации, не обеспечивая доступа к правосудию, процедурам обжалования, защиты или возмещения ущерба.
81. В соответствии с общими правилами международной торговли право конечных потребителей на доступ к публично предлагаемым

программному обеспечению или услугам в киберпространстве, будь то бесплатно или за плату, не должно быть ограничено. Отказ в доступе к конкретным интернет-ресурсам противоречит всему объему «прав человека в Интернете»: доступ к информации, свобода выражения мнения, право на неприкосновенность частной жизни, право на образование и право на репутацию, а также право на достойную работу и другие экономические права. Оно также нарушает право на развитие и может привести к нарушению права на здоровье и даже права на жизнь в чрезвычайных ситуациях. Это представляет собой фактическую дискриминацию в отношении подпавших под санкции обществ. Это также противоречит неоднократным призывам Организации Объединенных Наций и других организаций к солидарности, сотрудничеству и многосторонности.

82. Несмотря на растущее применение односторонних санкций за «злонамеренную» деятельность в киберпространстве, правовая или гуманитарная оценка обычно не проводится. Следовательно, такие вопросы, как свобода выражения мнения и допустимость ограничений в соответствии со статьями 19 и 20 Международного пакта о гражданских и политических правах, а также гарантии соблюдения процессуальных прав, не рассматриваются.

83. Любые односторонние меры против деятельности средств массовой информации, социальных сетей и социальных платформ могут осуществляться только в том случае, если они не нарушают международных обязательств государств, в том числе в отношении свободы прессы, свободы доступа к информации и свободы выражения мнения, и только в том случае, если они соответствуют статьям 19 и 20 Международного пакта о гражданских и политических правах и другим нормам международного права, в целях, в частности, запрета пропаганды войны, геноцида, выступлений в пользу национальной, расовой или религиозной ненависти, представляющих собой подстрекательство к дискриминации, вражде или насилию; предотвращения распространения детской порнографии; уважения прав и репутации других лиц; или защиты государственной безопасности, общественного порядка, здоровья или нравственности населения, при условии соблюдения критериев добросовестности, разумности, необходимости и соразмерности. Бремя доказывания обоснованности соответствующих ограничений лежит на государстве; перенос бремени доказывания на пострадавшие средства массовой информации не соответствует международному праву.

Рекомендации

84. Односторонние санкции, введенные в связи со злонамеренной активностью с использованием киберсредств, должны быть пересмотрены и отменены, если они не соответствуют санкциям Совета Безопасности или не могут быть квалифицированы как законные меры возмещения или контрмеры. Никакие меры по обеспечению выполнения резолюций Совета Безопасности в киберсфере не могут быть приняты без четкого дополнительного разрешения Совета Безопасности.

85. Все критерии отнесения деятельности к государствам, компаниям и частным лицам должны соблюдаться в полном объеме. Никакие санкции не могут быть введены на основании секретной разведывательной информации.

86. Односторонние санкции не должны использоваться в качестве замены уголовных процессов в отношении киберпреступлений. Они не должны заменять бремя доказывания или использоваться при отсутствии юрисдикции. Должны быть соблюдены все надлежащие процессуальные и юрисдикционные нормы.

87. Государствам следует принимать меры в ответ на злонамеренную активность с использованием киберсредств только при наличии достаточных доказательств и при проведении правовой оценки с учетом положений международного права, международного гуманитарного права и права прав человека.

88. Соблюдение прав человека должно быть гарантировано каждому человеку в мире без какой-либо дискриминации. Никакие «благие намерения или цели» не могут оправдать косвенный или непреднамеренный охват всего населения страны односторонними санкциями, который приводит к человеческим страданиям и «сопутствующим потерям», ибо это является нарушением основных прав человека.

89. При введении санкций против государственных органов и должностных лиц должен в полной мере соблюдаться принцип суверенного равенства государств и юрисдикционные иммунитеты государств и их собственности. Отступление от международно-правовых норм и стандартов в области прав человека на основании административной процедуры не допускается.

90. Медиа-платформы, компании по разработке программного обеспечения и предприятия, предоставляющие интернет-услуги, не обладают судебной компетенцией и должны действовать в полном соответствии с международными правовыми стандартами, выполняя обязательства по проявлению должной осмотрительности, чтобы гарантировать, что их деятельность не нарушает основные права человека, в частности свободу выражения мнения, в соответствии с Руководящими принципами предпринимательской деятельности в аспекте прав человека.

91. Совет Безопасности должен начать обсуждение, по крайней мере на уровне формулы Аррии, вопроса об использовании односторонних санкций в ответ на злонамеренную деятельность в киберпространстве, которая может рассматриваться как угроза международному миру и безопасности.

92. Контрмеры, принимаемые в ответ на злонамеренную киберактивность или активность с использованием киберсредств, должны полностью соответствовать требованиям закона о международной ответственности: пропорциональность; необходимость; соблюдение императивных норм международного права, основных прав и гуманитарных стандартов; и запрет на репрессалии.

93. Комитет по правам человека должен инициировать пересмотр своего замечания общего порядка № 34 (2011) о свободе мнений и их выражения, чтобы гарантировать, что современная практика введения односторонних санкций, в частности ограничений в отношении средств массовой информации, полностью соответствует стандартам, изложенным в статьях 19 и 20 Международного пакта о гражданских и политических правах, и

обеспечить, чтобы доступ к информации и академическое сотрудничество с участием ученых из стран, подвергшихся санкциям, включая возможность публикации исследований, не ограничивались произвольно по причине гражданства или местонахождения этих ученых.

94. Государствам не следует использовать онлайн-платформы для целевого воздействия на лиц, подозреваемых в совершении преступлений, путем распространения непроверенной и поэтому, возможно, ложной и клеветнической информации, которая может угрожать их жизни или повлиять на их репутацию, или предлагать денежное вознаграждение за информацию о них в связи с такой информацией.

95. Любые ограничения свободы выражения мнений в Интернете должны приниматься только в полном соответствии с требованиями статей 19 и 20 Международного пакта о гражданских и политических правах. Наличие информации из различных источников, с возможностью проверки и всесторонней оценки, является важным средством мирного урегулирования международных споров.
