United Nations A/77/296

General Assembly

Distr.: General
17 August 2022

Original: English

Seventy-seventh session
Item 69 (b) of the provisional agenda*
Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms

Unilateral sanctions in the cyberworld: tendencies and challenges**

Note by the Secretary-General

The Secretary-General has the honour to transmit to the General Assembly the report of the Special Rapporteur on the negative impact of unilateral coercive measures on the enjoyment of human rights, Alena Douhan, in accordance with Assembly resolution 76/161 and Human Rights Council resolutions 27/21 and 45/5.

* A/77/150.

** The present report was submitted after the deadline so as to include the most recent information.

Report of the Special Rapporteur on the negative impact of unilateral coercive measures on the enjoyment of human rights, Alena Douhan

Summary

In the present report, the Special Rapporteur on the negative impact of unilateral coercive measures on the enjoyment of human rights, Alena Douhan, provides an overview and assessment of the development of cybertechnologies and their impact on the use of unilateral sanctions, assesses the legality and humanitarian impact of measures taken by States and regional organizations with reference to malicious activity in cyberspace, and pays special attention to the blocking of access to web pages and software.

I. Introduction

1. The present report is submitted to the General Assembly pursuant to its resolution 76/161 and Human Rights Council resolutions 27/21 and 45/5, in which the Special Rapporteur on the negative impact of unilateral coercive measures on the enjoyment of human rights, Alena Douhan, was requested to, inter alia, gather all information relevant to the negative impact of unilateral coercive measures on the enjoyment of human rights; to study relevant trends, developments and challenges; and to make guidelines and recommendations on ways and means to prevent, minimize and redress their adverse impact on human rights; as well as to draw the attention of the Assembly, the Council and United Nations High Commissioner for Human Rights to relevant situations and cases.

2. The Special Rapporteur has taken note of the accelerating expansion of unilateral sanctions involving cybermeans or in cyberspace, resulting, inter alia, in new interpretations of the notion of unilateral sanctions. Recognizing the ambiguous nature of the notion of cybersanctions, she seeks to identify how the development of cybertechnologies has affected the use of unilateral sanctions by individual States and how human rights are affected. The present report contains an overview and assessment of: the expansion of unilateral sanctions in the cyberarea; how States react to "malicious" activity, and legal problems with the reactions; the development of national legislation; the humanitarian impact of measures imposed; the prevention of access to online banking; defamation campaigns and threats with sanctions as part of sanctions regimes; the blocking of access to online platforms and services; and other sanctions and sanctions-related activity in the cybersphere.

3. For the purposes of the present report, the Special Rapporteur issued a call for submissions from States, United Nations specialized agencies, regional organizations, human rights institutions, civil society, scholars, research institutions and others about unilateral sanctions in the cyberworld. [1] Responses were received from the Governments of Belarus, Cuba, Iran (Islamic Republic of), the Russian Federation, the Syrian Arab Republic and Zimbabwe. Responses were also received from the United Nations country team in the Syrian Arab Republic and a number of non-governmental organizations, civil society organizations, business enterprises, academics and concerned individuals. The Special Rapporteur expresses her gratitude to all respondents.

4. The Special Rapporteur seeks to align the use of the term "cybersanctions" with the way sanctions are traditionally defined, which is on the basis of the instruments used (economic, financial or military) or the target (sectoral or targeted). She also notes that any reference to the existence of authorization to impose cybersanctions is not grounded in international law.

5. The Special Rapporteur recognizes the existence of multiple reports of Internet shutdowns and limitations on Internet access imposed by Governments. This issue, however, does not fall within the scope of the mandate. In the present report, the Special Rapporteur therefore focuses on the use of unilateral sanctions by States and regional organizations and overcompliance as they relate to cybertechnologies.

6. The Special Rapporteur emphasizes that this assessment of unilateral sanctions in the cyberarea shall not be viewed as a ground for their legalization or legitimization. Any unilateral measures without or beyond the authorization of the Security Council that cannot be qualified as retorsions or countermeasures are illegal under international law and constitute unilateral coercive measures, which have been

[1] The call for submissions is available at www.ohchr.org/en/calls-for-input/calls-input/call-input-reports-secondary-sanctions-civil-and-criminal-penalties.

condemned in numerous resolutions of the Human Rights Council and the General Assembly. The development of cybertechnologies results in the need to assess these new types of measures as concerns their legality.

II. "Malicious" use of cybertechnologies as a ground for introducing unilateral sanctions

7. The Special Rapporteur is mindful of changes and challenges introduced by cybertechnologies to all areas of life. She also acknowledges that private actors' cyberactivity can constitute a threat to the maintenance of international peace and security [2] through transboundary crimes, including international terrorism; [3] war crimes, crimes against humanity or genocide;[4] hostile propaganda;[5] defamation; or hostility to Governments, companies or individuals. She admits that, under certain conditions, a cyberoperation may constitute an armed attack or part of an armed attack[6] or be part of a military operation in the course of a non-international military conflict.[7]

8. The Special Rapporteur underscores that, as of July 2022, the Security Council had imposed targeted sanctions with reference to malicious cyberactivity only once – against individuals and organizations in Yemen that were responsible for attacks with drones and unmanned boats.[8] In all other cases, the Security Council referred to the primary obligation of States to suppress terrorist activity in the cyberarea; to guarantee the security of their citizens in the face of terrorism, including by controlling information flows; to control cryptocurrency transactions so as to prevent money-laundering and terrorist financing;[9] to control passenger information among airlines;[10] and to investigate terrorist crimes. The Organization for Security and Cooperation in Europe (OSCE) refers in such cases to the obligation of States to guarantee all standards of due process.[11]

---

[2] Security Council resolution 2462 (2019), preamble and paras. 19 and 21; Security Council resolution 2419 (2018), preamble; Security Council resolution 2490 (2019), preamble; General Assembly resolution 72/246, paras. 7–8; United Nations Office on Drugs and Crime, *The Use of the Internet for Terrorist Purposes* (Vienna, 2012), pp. 3–11 and 32–34; and A/70/174, para. 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] Security Council resolution 2490 (2019), preamble.

[5] Eric de Branbandere, "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, available at 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, available at https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=BAA341028EBFF1E8C12563CD00519E66.

[8] Security Council resolution 2140 (2014), paras. 11–19; Security Council resolution 2216 (2015), paras. 14–19; and S/2021/79, paras. 62–70.

[9] Security Council resolution 2462 (2019), para. 19.

[10] Security Council resolution 2482 (2019), para. 15 (c).

[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, available at www.osce.org/files/f/documents/7/e/299091.pdf.

9. At the same time, the Special Rapporteur notes the absence of a common understanding of the term "malicious" as concerns cyberactivity, and its arbitrary use by States.[12] She emphasizes that possible responses to malicious activity in cyberspace cannot have a generic character and that they depend on the qualification of each act.

10. The Special Rapporteur notes that the State practice of imposing sanctions in response to real or alleged malicious cyberactivities is rather extensive. In particular, Executive Order No. 13694 of 1 April 2015 of the United States of America, as amended by later documents,[13] introduced a list of cyberenabled activities subject to sanctions,[14] which included, inter alia, attacks on critical infrastructure, interference in the election process,[15] disruption of networking or computer operations, and misappropriation of financial funds and personal information. Subsequently added were substantial destructive virus attacks, the prevention of access to systems,[16] the gaining of unauthorized access to election and campaign infrastructure, the covert distribution of propaganda and disinformation,[17] efforts to undermine democratic institutions in the United States and its allies and partners, efforts to engage in and facilitate malicious cyberenabled activities against the United States and its allies and partners, efforts to foster and use transnational corruption to influence foreign Governments, and efforts to pursue extraterritorial activities targeting dissidents or journalists.[18]

11. Reportedly, during the period 2011–2021 the United States designated 303 natural and legal persons from 10 States with reference to various types of malicious cyberactivity.[19] For example, two State organs, 46 citizens and 13 companies of the Russian Federation and Ukraine were listed with reference to interference in elections.[20]

12. The Special Rapporteur notes that some of these measures are taken by the United States with reference to implementing Security Council resolutions concerning the Democratic People's Republic of Korea,[21] to suppress attempts by the

[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] For example, United States, Executive Order No. 13757 of 28 December 2016 on taking additional steps to address the national emergency with respect to significant malicious cyberenabled activities.

[14] United States, Executive Order No. 13694 of 1 April 2015 on blocking the property of certain persons engaging in significant malicious cyberenabled activities. See also 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, available at https://home.treasury.gov/system/files/126/cyber.pdf.

[16] United States, Countering Russian Influence in Europe and Eurasia Act of 2017, as amended, para. 224.

[17] United States, Executive Order No. 13848 of 12 September 2018 on imposing certain sanctions in the event of foreign interference in a United States election.

[18] United States, Executive Order No. 14024 of 15 April 2021 on blocking property with respect to specified harmful foreign activities of the Government of the Russian Federation.

[19] Jason Bartlett and Megan Ophel, "Sanctions by the numbers: spotlight on cyber sanctions", Center for a New American Security, 4 May 2021; list of United States documents concerning the sanctions adopted with reference to malicious cyberactivity up to 2020, available at https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/sanctions-related-to-significant-malicious-cyber-enabled-activities; and 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, available at https://sgp.fas.org/crs/row/R45415.pdf.

[21] See, for example, Security Council resolutions 1718 (2006) and 2397 (2017).

Democratic People's Republic of Korea to use cybertechnologies to circumvent Security Council sanctions and additional United States sanctions.[22]

13. In its 2020 guidance on the cyberthreat posed by the Democratic People's Republic of Korea, the United States refers to disruptive or destructive cyberactivities affecting critical United States infrastructure. Such activities may be prosecuted by the United States, and secondary sanctions may be applied.[23] The United States also offers monetary rewards for information that leads to the disruption of financial mechanisms of persons engaged in certain activities that support the Democratic People's Republic of Korea, including money-laundering, the evasion of sanctions and cybercrime.[24]

14. The Special Rapporteur notes that a panel of experts established by the Security Council[25] discussed the evasion of financial sanctions by the Democratic People's Republic of Korea through cybermeans[26] and recommended that the Security Council consider addressing that situation in any future sanctions.[27]

15. Since 2019, the European Union and the United Kingdom of Great Britain and Northern Ireland have applied measures referring to serious or attempted cyberattacks, understood as actions involving access to information systems, information systems interference, data interference or data interception.[28] Cyberattacks constituting a threat to the European Union are understood broadly and include "those carried out against its institutions, bodies, offices and agencies, its delegations to third countries or to international organizations, its common security and defence policy operations and missions and its special representatives". Both the European Union and the United Kingdom have introduced visa and entry prohibitions and requested the freezing of assets of listed persons or the refusal to make assets or funds available to them.[29]

16. As a result, in 2020 eight individuals and four legal entities from China, the Democratic People's Republic of Korea and the Russian Federation were listed for being considered to have provided support for or to have been involved in or facilitated cyberattacks or attempted cyberattacks, including the attempted cyberattacks against the Organisation for the Prohibition of Chemical Weapons and the cyberattacks publicly known as "WannaCry" and "NotPetya", as well as the one known as "Operation Cloud Hopper", and to have been involved in cyberattacks with a significant effect that constituted an external threat to the European Union or its member States, in particular, the cyberattack against the federal parliament of Germany in April and May 2015.[30]

---

[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] See the Rewards for Justice official website of the Government of the United States, available at https://rewardsforjustice.net/english/about-rfj/north_korea.html.

[25] See Security Council resolution 1874 (2009), para. 26 and Security Council resolution 2515 (2020), para. 1.

[26] S/2019/691, paras. 57–71 and S/2021/211, paras. 126–129.

[27] S/2019/691, recommendations 8–11; and S/2020/151, recommendations contained in annex 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). Until 31 December 2020, the United Kingdom applied the European Union cybersanctions.

[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.

17. Following The decision by the United Kingdom to leave the European Union, or "Brexit", the United Kingdom adopted a regulation on cybersanctions[31] providing for unilateral sanctions against the same persons identified in the European Union list.[32] The Special Rapporteur notes with regret that neither a legality assessment nor a humanitarian impact assessment was carried out while drafting the regulation.[33]

18. Amendments made to the Australian Autonomous Sanctions Act in 2021 provide for the possibility of unilateral sanctions in response to "malicious activity in cyberspace".[34] No sanctions of this type had been imposed by Australia as of July 2022.

19. The Special Rapporteur notes with concern the new tendency among a number of States to withdraw the licences of media outlets; remove goods, services or content online; or provide for criminal or civil liability because of sanctions-related activity in cyberspace.

20. She is mindful in particular of the discussion by the European Union of the Digital Services Act, which is aimed at establishing "rules for the removal of illegal goods, services or content online" and obligations of platforms "to take risk-based action to prevent abuse of their systems",[35] supplementing the European Democracy Action Plan. The Plan sets out measures to promote free and fair elections, strengthen media freedom and counter disinformation. The latter is understood to be false or misleading content shared with or without harmful intent, as well as information to influence operations and foreign interference in the information space.[36] In the guidance on strengthening the code of practice on disinformation presented by the European Commission in 2021, disinformation is understood extremely broadly and is defined as including disinformation, misinformation, information influence operations and foreign interference in the information space, including from foreign actors, where information manipulation is used with the effect of causing significant public harm.[37]

21. The Special Rapporteur is also mindful that this de facto allows for the public surveillance of social networks and for requests that the platforms remove relevant tweets, blogs and private messaging services. Meanwhile, public harm is also viewed very broadly and is defined as including the "real and foreseeable negative impact on public health, public security, civil discourse, political participation and equality".[38] Large platforms shall consider "the possible negative impacts of systemic risks on

[31] United Kingdom, Cyber (Sanctions) (EU Exit) Regulations 2020 No. 597 of 17 June 2020, available at www.legislation.gov.uk/uksi/2020/597/made.

[32] Iryna Bogdanova and María Vásquez Callo-Müller, "Unilateral cyber sanctions: between questioned legality and normative value", *Vanderbild Journal of Transnational Law*, vol. 54 (2021).

[33] See United Kingdom, Explanatory Memorandum to the Cyber (Sanctions) (EU Exit) Regulations 2020 No. 597, available at www.legislation.gov.uk/uksi/2020/597/pdfs/uksiem_20200597_en.pdf.

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

[35] European Commission, "Europe fit for the digital age: Commission proposes new rules for digital platforms", 15 December 2020, available at 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.

society and democracy, such as disinformation or manipulative and abusive activities",[39] which is interpreted as including "State-disseminated falsehoods".[40]

22. The Special Rapporteur notes with concern that the above tendency is seen in recent sanctions imposed by Australia, Canada,[41] the United Kingdom[42] and the United States, as well as by the European Union, withdrawing permissions of some media outlets of the Russian Federation in 2022 (Sputnik and RT), citing as grounds those outlets' policies of reflecting the position of the Russian Federation on the conflict in Ukraine, disinformation, foreign interference and influence operations, "propaganda actions targeted at civil society in the Union and neighbouring countries, gravely distorting and manipulating facts", and actions that constituted a "significant and direct threat to the Union's public order and security".[43] The same tendency is also seen in the designations of numerous journalists from State media. Certain limitations have also been imposed in other countries. Some European Union countries have limited the access to a larger list of television channels of the Russian Federation.[44]

23. The Special Rapporteur is concerned that, although the need to adhere to the freedom of expression is acknowledged in the above-mentioned documents, justifications are made for the limitations by stating that the media outlets are controlled by the Russian Federation, but no assessment is made in accordance with articles 19 and 20 of the International Covenant on Civil and Political Rights.

24. At the same time, the consequent decision of the Russian Federation to limit broadcasting and online access to the BBC, Voice of America, Deutsche Welle, Meduza and other media outlets has been condemned by the European Union as limiting freedom of expression,[45] despite the existing report on the use of unverified information in the reports about the conflict in Ukraine.[46] The United States presented similar objections after the Russian Federation blocked access to Instagram and Facebook because of the criminal case against the Meta company under articles 205.1 and 280 of the Criminal Code of the Russian Federation on charges of enhancing extremism and terrorism.[47]

III. Sanctions on trade in and access to software and online platforms

25. The Special Rapporteur is mindful of the reported expansion of problems with the availability of software and access to online platforms. Trade in software is often

[39] Ibid., para. 68.

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

[41] France 24, "YouTube blocks Russian state-funded media, including RT and Sputnik, around the world" 12 March 2022 and 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] See 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] TASS Russian News Agency, "US State Department condemns Russia's decision to recognize Meta as extremist organization", 22 March 2022, available at https://tass.com/world/1425401.

limited as part of a sanctions regime. In particular, by 2010 the European Union had already imposed restrictions on the transfer of software, notably that which could have military and civilian dual use.[48] The Special Rapporteur acknowledges that the European Union regulations provide for substantial lists of exemptions, including software in the public domain that end users can obtain from retailers and install without outside support.[49]

26. The United States has expanded the list of restrictions on the trade of software to include "technology, and software relating to materials processing, electronics, telecommunications, information security, sensors and lasers, and propulsion," including traditional encryption and geospatial software.[50] This causes companies developing software under United States jurisdiction to be concerned about complying with sanctions regimes regarding trade in software provided through public offers, used for private purposes and sometimes even at no cost,[51] to a number of countries, including (as of 2017) the Balkan countries, Belarus, Cote d'Ivoire, Cuba, the Democratic People's Republic of Korea, the Democratic Republic of the Congo, Iran (Islamic Republic of), Iraq, Lebanon, Libya, Myanmar, Somalia, the Sudan, the Syrian Arab Republic[52] and Zimbabwe, and also to become extremely concerned about the growing level of software piracy.

27. Because of the prohibition on technology exports, the Syrian Arab Republic has been unable to buy software made only by United States companies for X-ray computed tomography scanners and ventilators[53] used in treating the coronavirus disease (COVID-19), as well as for maintenance of other vital services.[54] Zimbabwe has reported that gaining access to necessary software can require going through intermediaries or substantially raising costs, or that access does not exist at all because providers decline to sell it to Zimbabwe or because payments may be intercepted.[55] The same problem applies with regard to equipment for government services; the Islamic Republic of Iran has reported problems with buying software for medical equipment and for equipment to monitor for earthquakes.[56]

28. The Special Rapporteur underlines that even the United Nations' own offices face challenges when procuring IT equipment and software in countries under sanctions.[57]

29. She is also mindful of the effects of compliance and overcompliance with sanctions by the private sector. Because of the fear of secondary sanctions, companies

[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; and 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] Gibsonn 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] Submission by Syrian Arab Republic.

[53] Note 100/20 of the Permanent Mission to the United Nations of Syrian Arab Republic and submission by Zimbabwe.

[54] Submission by Syrian Arab Republic.

[55] Submission by Zimbabwe.

[56] Report on the country visit to Islamic Republic of Iran (forthcoming).

[57] Confidential submission.

under United States jurisdiction are reported to comply with limitations concerning the software traditionally used for regular administration and public and private purposes, in particular for commercial Internet services or connectivity,[58] and even for non-commercial activity.

30. The United States Department of the Treasury's Office of Foreign Assets Control decides on a case-by-case basis whether offering specific services violates United States sanctions. It has been reported that, thus far, GitHub is the only high-profile technology company to have acquired a licence to offer previously restricted services to Iranians – an onerous process that took two years, according to GitHub.[59] The lack of clarity around applications and the lengthy and arduous process, as well as potential additional costs, are likely to discourage other technology platforms from seeking such licences.[60]

31. The Special Rapporteur thus notes with regret the growing number of measures preventing citizens of countries under sanctions from having access to online platforms for scholars and professionals (including medical staff).[61] It has been reported that at least 300 companies have restricted access to their services by Iranian users as of July 2020.[62] Videoconference services such as Zoom,[63] the majority of Google services, as well as educational resources or services tied to the work surrounding education, such as Udemy,[64] Amazon Cloud, GoDaddy, GoFundMe, Khan Academy, Coursera, GitLab, Slack and Digital Ocean, are no longer being provided to Iranians.[65] Some international cloud providers, such as Digital Ocean, are reported to have stopped providing hosting to Iranian private sector services on short notice, making them more dependent on other platforms and domestic systems.[66]

32. Zoom and some other platforms were not available to residents and citizens of a number of countries under sanctions, including for teaching purposes or even for communication among doctors to discuss symptoms, diagnostics and means of treatment, including in relation to COVID-19. Limitations in the Zoom service agreement have expanded substantially since 2020.[67] This has made it impossible to use Zoom even for United Nations communications as initially planned. Cuba, in particular, was unable to participate in a Zoom summit meeting of the Organization of African, Caribbean and Pacific States in 2020 to discuss the COVID-19 pandemic.[68]

---

[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] Report to the Human Rights Council.

[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, available at https://filter.watch/en/2021/03/12/policy-monitor-february-2021.

[64] Submission on behalf of the Miaan Group.

[65] Submission by Islamic Republic of Iran.

[66] Submission on behalf of the Miaan Group and submission by Syrian Arab Republic.

[67] Zoom, "Zoom terms of service", 13 April 2022, available at https://explore.zoom.us/en/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, available at www.granma.cu/hilo-directo/2020-06-05/hilo-05-06-2020-00-06-14.

33. The Special Rapporteur has been informed that students, scholars and professionals from countries under sanctions face problems in gaining access to professional databases. In particular, Iranian and Syrian doctors could not get access to the PubMed medical database after its server had been transferred to Google.[69] In many cases, they cannot register for databases owing to the absence of their nationality in the lists of countries where the service is available or owing to the rejection of residents and nationals of countries under sanctions. This results in discrimination, the isolation of scholars and professionals, and the impossibility of gaining access to knowledge (according to reports from Iran (Islamic Republic of),[70] Syrian Arab Republic[71] and Zimbabwe[72]). Subscriptions to online services are also impeded, as sanctions impede payments.

34. Some reports also reflect growing overcompliance by e-commerce platforms on the basis of the suspected existence of any relation to the countries under sanctions. For example, Etsy removed "Persian dolls" listed for sale on the platform, despite the dolls being made in and with material from the United States, according to a user in 2020.

35. The Special Rapporteur also notes with concern that scholars from targeted countries (Iran (Islamic Republic of), Russian Federation, Syrian Arab Republic and Venezuela (Bolivarian Republic of)) are reported to be prevented by the introduction of "sanctions clauses" from the very possibility of submitting their articles for publication, including in online journals, owing to their nationality.[73,74] This results in the isolation of people engaged in art, science and sport.[75]

36. She is also mindful of the expanding practice among online providers of closing online accounts, blogs and channels of designated and non-designated individuals and companies. Blocking social media accounts is done in particular by companies registered in the United States as part of the Magnitsky sanctions regime.[76]

37. It has also been reported that, in 2021, a number of YouTube channels and accounts held by Belarusian media were blocked and journalists were designated.[77] Twitter, YouTube, Spotify, TikTok and Meta have blocked accounts held by media of the Russian Federation considered to be associated with the State. Google and Instagram downgraded references to media of the Russian Federation in search results, which reduced access to these media by 90 per cent.[78] Meta has imposed restrictions with reference to the spread of fake news from the Russian Federation and Belarus through the use of false social media accounts.[79]

---

[69] Responses and comments from Islamic Republic of Iran.

[70] Report on the country visit to Islamic Republic of Iran (forthcoming).

[71] Submission by Syrian Arab Republic.

[72] Submission by Zimbabwe.

[73] Report on the country visit to Islamic Republic of Iran (forthcoming) and 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; OTH 37/2022; OTH 38/2022; OTH 39/2022; and OTH 40/2022, available at https://spcommreports.ohchr.org/TmSearch/Mandates?m=263.

[75] Submission by Syrian Arab Republic.

[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, available at https://edition.cnn.com/2020/01/10/tech/instagram-iran-soleimani-posts/index.html and Jonny Tickle, "Chechen leader Kadyrov banned from Instagram again, loses account with 1.4 million followers", RT, 13 May 2020, available at www.rt.com/russia/488533-kadyrov-banned-instagram-again/.

[77] Submission of Belarus.

[78] See 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.

IV. Other aspects of the application of sanctions in the digital sphere

38. The Special Rapporteur also underlines that access to the Internet and information can be prevented by sanctions indirectly. Shortages of fuel in the Bolivarian Republic of Venezuela result in electricity shutdowns that quite often make access to the Internet impossible, while reduced income makes Internet access unfeasible for the majority of the population in the Syrian Arab Republic, Venezuela (Bolivarian Republic of),[80] Zimbabwe and many other countries.[81]

39. The unavailability of necessary equipment, spare parts and software, and of financial transactions involving them, results in shrinking coverage areas for Internet communications. In particular, Internet coverage in the Bolivarian Republic of Venezuela has decreased from 50 to 90 per cent coverage in 2015, before sanctions, to 10 per cent.[82] In the Syrian Arab Republic, fixed communication services decreased by 38 per cent; mobile Internet coverage by 15 per cent and Internet coverage by 7 per cent.[83]

40. The Special Rapporteur is also concerned by threats and public accusations on the Internet that individuals or companies, either designated or non-designated, are engaged in criminal activity. She is especially mindful about offers of rewards made by the United States on the official Rewards for Justice website and Twitter account for locating individuals allegedly involved in terrorist activity, without any legal cases being initiated against them.[84]

41. Quite often countries facing serious economic sanctions develop their own cryptocurrency (e.g. Democratic People's Republic of Korea and Venezuela (Bolivarian Republic of)). The United States now imposes sanctions for using these cryptocurrencies in transactions.[85]

V. Legal assessment of the use of unilateral sanctions in the cybersphere and their humanitarian impact

42. The Special Rapporteur regrets that a legal assessment of the use of sanctions and other types of enforcement action in response to malicious activity is usually not carried out and that the notion of "maliciousness" does not have any uniform definition.

43. The International Committee of the Red Cross (ICRC) states that, to be qualified as an armed attack, the use of cybertechnologies must endanger the very existence of a State;[86] cause the loss of human lives (death or injury of combatants or civilians), or destruction of or damage to property (civilian or military), including critical

[80] A/HRC/48/59/Add.2.
[81] Submission by Access Now.
[82] A/HRC/48/59/Add.2.
[83] Submission by Syrian Arab Republic.
[84] See communication USA 9/2021, available at 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).

infrastructure,[87] or the loss of part of a State's territory;[88] have a causal link to the immediate negative consequences (with a time frame of seconds or minutes between the attack and its results);[89] and be attributable to a specific State under the law of international responsibility. The Special Rapporteur underlines that only attacks which meet the above criteria can give rise to acts of self-defence, in accordance with Article 51 of the Charter of the United Nations.

44. She also underscores that "attacks on critical infrastructure" may be understood in various ways and may be interpreted to include attacks against dams, nuclear power stations, arms control systems, bank accounts and operations, gas and oil pipelines, electricity lines, taxation systems, governmental servers and computer networks,[90] as well as other critical infrastructure, and the interception of control over air defence systems,[91] floodgates of dams, aircraft or trains (which can cause them to collide).[92] In particular, the Islamic Republic of Iran refers to a 2021 attack that halted the operation of more than 4,300 gas stations (roughly 70 per cent of all gas stations in the country), resulting in tens of millions of Iranians being unable to gain access to fuel. The Islamic Republic of Iran also refers to the 2010 Stuxnet attack, which was introduced by a belligerent supplier through a centrifuge platform in the Natanz Nuclear Reactor.[93]

45. The Special Rapporteur wishes to highlight that the regime of fighting international terrorism in cyberspace is identified in Security Council resolutions that oblige States to take a broad range of measures to prevent the use of cybertechnologies for the dissemination of hostile propaganda, incitement to violence, money-laundering and the financing of terrorism, the justification of terrorist activities and ideology, involvement in terrorist activities, and the planning and commission of terrorist acts.[94]

46. She underlines that measures to implement Security Council resolutions, including the designation of specific individuals and companies for malicious cyberactivity, can be implemented only in full conformity with the authorizations

[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).

[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 Dinniss, *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, available at https://ila.vettoreweb.com/Storage/Download.aspx?DbStorageId=1055&StorageFileGuid=c911005c-6d63-408e-bc2d-e99bfc2167e4.

[92] 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, para. 437.

[93] Submission by Islamic Republic of Iran.

[94] Security Council resolution 2462 (2019), preamble and paras. 19 and 20 and Security Council resolution 2419 (2018), preamble.

given, and that the imposition of additional unilateral sanctions [95] or other enforcement measures when the Security Council decisions are not observed[96] has no ground in international law.

47. The Special Rapporteur thus wishes to point out that States can take unilateral measures in response to malicious cyberactivity only if they do not breach any international obligations, including in the sphere of human rights (retortions), or if their wrongfulness is excluded in accordance with international law in the course of countermeasures.[97]

48. Countermeasures can be taken by injured States only in response to the violation of a specific international obligation by a specific State and may be directed only against that State[98] to induce it to comply with the obligation in accordance with the principles of necessity and proportionality to the violation and prohibitions on violating peremptory norms of international law, using force, taking unauthorized reprisals or violating fundamental human rights.[99] To legally take countermeasures, a State must be able to prove the existence of the alleged perpetrator's "effective"[100] or "overall"[101] control over the malicious cyberact.

49. The Special Rapporteur agrees in this regard with the position taken by the drafters of the Tallinn Manual 2.0, namely, that the same rules of attribution of the activity of non-State actors to States (acting under their direction and control) shall be applied to activity in the cybersphere, as international law does not provide any additional or different regulation.[102] Countermeasures thus cannot also be applied to natural or legal persons accused of committing cybercrimes.[103]

---

[95] Vera Gowland-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; and Christian Schaller, "Massenvernichtungswaffen und präventivkrieg – möglichkeiten der rechtvertigung einer militärischen intervention im Irak aus völkerrechtlicher sicht", *German Yearbook of International Law*, vol. 62 (2002), p. 654.

[97] See 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] Articles on responsibility of States for internationally wrongful acts, arts. 48–51. Dorothee Geyrhalter, for example, claims that it is possible for economic sanctions to be applied against States responsible for mass violations of fundamental human rights; see Geyrhalter, *Friedenssicherung durch Regionalorganisationen ohne Beschluß des Sicherheitsrates*, p. 66. See also Antonios Tzanakopoulos, "State responsibility for 'targeted sanctions'", *American Journal of International Law*, vol. 113 (2019), pp.136–137.

[100] International Court of Justice, *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America), merits, judgment of 27 June 1986, paras. 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.

[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.

50. The Special Rapporteur wishes to point out that the use of unilateral sanctions against State bodies and officials does not comply with the principle of sovereign equality of States or with provisions on the immunities of States and their property, especially when sanctions lead to the seizure of property of State-controlled companies. She underlines that the immunity of States and their property is absolute. Since an administrative decision provides even fewer guarantees than a judicial process, the refusal to grant immunity on the basis of such a decision violates international law.

51. In this regard, the provision contained in article 1, paragraph 6, of Council of the European Union Regulation No. 2019/796 of 2019 does not meet the requirement set out in article 49, paragraph 1, of the articles on responsibility of States for internationally wrongful acts, as it refers to imposing sanctions "where deemed necessary to achieve common foreign and security policy objectives" rather than in response to an internationally wrongful act. Moreover, the provision allowing for the application of restrictive measures "in response to cyber-attacks with a significant effect against third States or international organizations" rather than the European Union or its member States does not refer to the obligations allegedly violated having an *erga omnes* character and goes counter to article 48 of the articles on responsibility of States for internationally wrongful acts.

52. Some publicists note that the relevant European Union regulation is aimed at providing the Union with financial levers in order to punish cyberattacks directly, more harshly and effectively.[104] It is noted that sanctioning States prefer this approach over criminal prosecution. In practice, it is difficult to comply with the burden of proof and due process requirements regarding cyberattacks,[105] but the Special Rapporteur underscores that sanctions cannot be punitive[106] and must be aligned with international legal standards.

53. The Special Rapporteur is also concerned that, even when unilateral sanctions are imposed on individuals and companies for actions in cyberspace and there is no evidence of their attribution to a particular State, they are still presented as sanctions against States (such as in the Countering Russian Influence in Europe and Eurasia Act and the Countering America's Adversaries through Sanctions Act, both promulgated by the United States).[107]

54. While recognizing that States are obliged to take measures to suppress cybercrimes against the State, its nationals and legal entities, such measures shall remain within the recognized international framework: joining international treaties, developing legislation, starting criminal investigations and prosecutions, and engaging in judicial cooperation.[108] The Special Rapporteur stresses that such measures shall be taken only if international and national human rights standards are fully observed.

55. Contemporary practice demonstrates, however, that individuals are designated with reference to the commission of cybercrimes against the State, citizens of the

[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] See also Office of Foreign Assets Control, "North Korea Sanctions Program", updated 2 November 2016, p. 5, available at https://home.treasury.gov/system/files/126/nkorea.pdf.

[108] OSCE Decision No. 7/06 of 5 December 2006 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".

State or its legal entities by executive bodies, rather than by judicial authorities, which deprives them of access to justice and the right to due process. According to data obtained from confidential sources, decisions are made on the basis of classified information and are not disclosed. Moreover, even the possibility of appealing an entry on a United States sanctions list is very limited, while the process is lengthy and costly. As a result, the person loses the opportunity to defend his or her rights in court, and the person's property rights, freedom of movement, right to protection of personal life and right to reputation, as well as economic, labour and social rights, are therefore violated.

56. The recent practice of the United States is notable in this regard. In 2020, six Nigerians were listed by the Office of Foreign Assets Control for stealing over 6 million dollars from victims across the United States through fraud involving cyberschemes.[109] A press release provides information about the alleged activity of each of the individuals, their photos and other personal data, as well as the presumed fraudulent schemes, as if they were confirmed facts. The same approach was taken towards two Russian nationals in 2020.

57. It is thus not clear why no criminal case has been initiated in response to the alleged cybercrimes. Instead, measures were taken in the form of unilateral sanctions upon the decision of the executive body, the Office of Foreign Assets Control, without any mention of the initiation of criminal proceedings or any possibility for the listed individuals to gain access to courts to protect their rights, reputations or personal data.

58. Moreover, the imposition of economic sanctions and entry bans, in addition to violating property rights and other rights, also runs counter to the requirement of the presumption of innocence set forth in article 14, paragraph 2, of the International Covenant on Civil and Political Rights, which is viewed by the Human Rights Committee as a guarantee "that States parties must respect, regardless of their legal traditions and their domestic law."[110] In paragraph 30 of its general comment No. 32 (2007) on the right to equality before courts and tribunals and to a fair trial, the Committee expressly notes that the presumption of innocence guarantees that "no guilt can be presumed until the charge has been proved beyond reasonable doubt" and "ensures that the accused has the benefit of doubt", and the Committee requests Governments to abstain from making public statements affirming the guilt of the accused. In its general comment No. 16 (1988) on the right to privacy, the Committee refers to the obligation of States not only not to infringe the honour and reputation of individuals but also to provide adequate legislation to guarantee their protection.[111] The Special Rapporteur notes with concern that none of the above requirements are observed when sanctions are imposed with respect to cybercrimes.

59. As a result, the expansive distribution of negative information about individuals and companies while bypassing the presumption of innocence and due process guarantees reduces, inter alia, their attractiveness for investors and counterparties, resulting in overcompliance with sanctions regimes.

60. Article 275 of the Treaty on the Functioning of the European Union provides for the possibility of appealing the imposition of sanctions to the Court of Justice of the European Union,[112] but the Court usually focuses on assessing the provision of

[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, available at: https://home.treasury.gov/news/press-releases/sm1034.

[110] Human Rights Committee, general comment No. 32 (2007) on the right to equality before courts and tribunals and to a fair trial, para. 4.

[111] Human Rights Committee, general comment No. 16 (1988) on the right to privacy.

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

minimum procedural guarantees and avoids the issue of property rights as subject to restriction under certain conditions,[113] as well as issues of presumption of innocence and reputational risks. To date, there have been no statements issued on the revision of sanctions imposed with reference to malicious actions in the information space.

61. The Special Rapporteur notes that the promise of rewards offered on the United States Rewards for Justice website and Twitter account for locating individuals allegedly involved in terrorist activity without any case being initiated against them, and quite often without information being properly verified,[114] not only ruins their reputation but may endanger their lives.

62. The Special Rapporteur underlines that the obligation of States to guarantee equal participation in academic cooperation and access to information and the right to benefit from scientific progress is reflected by the Committee on Economic, Social and Cultural Rights in its general comment No. 36 (2020) on science and economic, social and cultural rights.[115] Preventing nationals or residents of a specific country from having access to professional databases or platforms, from using these platforms for teaching or communication, or from submitting manuscripts for publication owing to their nationality or place of residence therefore constitutes discrimination on the ground of nationality or place of residence and results in the violation of the rights of access to information and freedom of communication and academic freedoms. Violations of the right to education have also been cited in Iran (Islamic Republic of), the Sudan and Venezuela (Bolivarian Republic of) because of the impossibility of using online platforms for educational purposes.

63. The Special Rapporteur underlines that access to Internet technologies and Internet resources have been referred to as an inalienable element not only of the struggle against the pandemic but also of the right to development.[116] The same approach has been taken by the Human Rights Council[117] and by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.[118] In its declaration on freedom of communication on the Internet, the Committee of Ministers of the Council of Europe called upon member States to "foster and encourage access for all to Internet communication and information services on a non-discriminatory basis, at an affordable price" (principle 4).[119]

64. The Declaration of Principles – Building the Information Society: a global challenge in the new Millennium calls for States to ensure access to information and communication infrastructure and technologies, information and knowledge for all[120] and considers information and communications technology to be the means of promoting the Millennium Development Goals.[121]

65. The Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance correctly noted in her report to the Human Rights Council in 2020 that people from the least developed countries had only one fourth

[113] Bogdanova and Callo-Müller, "Unilateral cyber sanctions", p. 938.
[114] See communication USA 9/2021, available at https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=25985.
[115] Committee on Economic, Social and Cultural Rights, general comment No. 36 (2020) on science and economic, social and cultural rights, paras. 21 and 52.
[116] Social Forum, held on 8 October 2020.
[117] Human Rights Council resolution 32/13, preamble.
[118] A/66/290, paras. 45–75.
[119] Declaration adopted by the Committee of Ministers of the Council of Europe on 28 May 2003, available at www.osce.org/fom/31507?download=true.
[120] Declaration adopted by the World Summit on the Information Society, Geneva Phase, at its fifth plenary meeting, on 12 December 2003, paras. 19–28, available at www.itu.int/net/wsis/docs/Geneva/official/dop.html.
[121] Ibid., paras. 1 and 2.

of the opportunity to gain access to the Internet compared with people in other countries, because of poverty and the underdevelopment of digital infrastructure, which resulted in limitations of their access to public health information online and their readiness to make use of digital schooling, working and shopping platforms, which were especially important in the time of COVID-19.[122]

66. One should not speak about the possibility of choosing trade partners when one speaks about publicly offered paid or non-paid cybersoftware or services. Preventing people in targeted countries from having access to these services violates a number of human rights, including the rights to access to information, freedom of communication, education and decent work and other economic rights, and constitutes de facto discrimination against targeted societies, which constitute about 20 per cent of the world population.

67. Another legal and human rights concern of the mandate holder is the possibility of introducing limitations on the broadcasting of mass media in the Internet space. The Security Council has repeatedly pointed out that the dissemination of information can also be malicious in nature and incite hatred, outbreaks of extremism and radicalization of the population and can pose a threat to the maintenance of international peace and security,[123] while the dissemination of hostile propaganda can violate the provisions of articles 19 and 20 of the International Covenant on Civil and Political Rights.

68. In its general comment No. 36 (2018) on the right to life, the Human Rights Committee explicitly states that the dissemination of hostile propaganda and incitement to hostilities constitute a direct violation of the right to life.

69. The Human Rights Council emphasizes the importance of free, fair and balanced access to information[124] to ensure the right to development. Possible restrictions are provided for in a number of international treaties, including the International Covenant on Civil and Political Rights in its article 19, paragraph 3 and article 20, including: (a) propaganda of war; (b) statements in favour of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence;[125] (c) orders not to leave anyone alive;[126] (d) direct and public incitement to commit acts of genocide;[127] (e) distribution of child pornography;[128] (f) dissemination of racist and xenophobic materials through online means, threats and insults;[129] (g) denial, extreme minimization, approval or justification of genocide or crimes against humanity;[130] and (h) calls for the overthrow of the Government or involvement in terrorist activities.[131]

70. The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has repeatedly insisted that the burden of proving the

[122] A/HRC/44/57, para. 20.
[123] Security Council resolution 2462 (2019), paras. 19 and 21, and Kalliopi Chainoglou, "Psychological warfare", in *Max Planck Encyclopedias of International Law*, para. 3.
[124] Human Rights Council resolution 33/3, para. 6 (j).
[125] International Covenant on Civil and Political Rights, art. 20.
[126] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, art. 40.
[127] Convention on the Prevention and Punishment of the Crime of Genocide, art. 3.
[128] Council of Europe Convention on Cybercrime, art. 9.
[129] Additional Protocol to the Convention on Cybercrime, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems, arts. 3–5.
[130] Ibid., art. 6.
[131] de Branbandere, "Propaganda".

validity of restrictions lies with the State.[132] At the same time, restrictions should be interpreted as narrowly as possible in order to avoid abuse.[133]

71. In accordance with article 19, paragraph 3, of the International Covenant on Civil and Political Rights, it is also possible to impose restrictions to respect the rights and reputation of others, or to protect State security, public order, public health or morals. A similar approach is reflected in article 34 of the Constitution of the International Telecommunication Union. At the same time, any restrictions must be imposed solely on the basis of the law, in accordance with the Human Rights Committee's general comment No. 34 (2011) on the freedoms of opinion and expression, and with due respect for freedom of expression as a priority.[134]

72. The European Union documents authorizing the introduction of restrictions on the broadcasting of RT and Sputnik in the European Union contain a reference to the violation of security and public order and commitment to freedom of expression and are introduced by law.[135] At the same time, the regulations do not reflect any of the criteria developed by the Human Rights Committee in its general comments. The rationale for the adoption of the regulations was not announced in any other way. The attempt by RT France to challenge the introduction of the broadcasting ban and demand its removal as an interim measure was unfruitful before the Court of Justice of the European Union, which ruled that there was a lack of proof of the presence of humanitarian and social harm, for which the duty of proof lay with RT France.[136]

73. The Special Rapporteur also notes the existing issues of assessing the legality of the authority of operators of online platforms and their obligations under international law, especially the obligation to protect human rights.[137] As with other businesses, they must avoid infringing on the human rights of individuals, address adverse human rights impacts with which they are involved, and seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products, services or business relationships, in accordance with the Guiding Principles on Business and Human Rights (principles 11–13).

74. It is for this reason that the Special Rapporteur warns States against using social networks and mass media to carry out propaganda, spread unverified information or call for violence. For example, permission by Meta's social network Facebook to post materials calling for violence against Russian citizens and officials[138] amid the development of the 2022 crisis in Ukraine,[139] later revised,[140] violated articles 19 and 20 of the International Covenant on Civil and Political Rights and led to a surge of

[132] A/HRC/29/32, paras. 32–35 and A/67/357, paras. 41 and 45.
[133] A/66/290, para. 24 and A/67/357, para. 45.
[134] A/66/290, paras. 24–30 and 46.
[135] Council of the European Union Regulation No. 2022/350, para. 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, available at 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.

Russophobia in numerous countries; it was condemned by the High Commissioner for Human Rights and the Secretary-General.[141]

VI. Conclusions and recommendations

Conclusions

75. **Digital technologies are changing all aspects of human life and international law, including the scope, subjects, means and methods of international and unilateral sanctions. They are used, inter alia, as responses to cybermeans of terrorist financing and malicious cyberactivity, including attacks on critical infrastructure not reaching the level of an armed attack, while some sanctions focus on the cyberworld by, inter alia, preventing access to public online platforms, blocking trade in software or in information and communications equipment, blocking social media accounts and listing cryptocurrencies.**

76. **This raises numerous concerns in international law, including the law of international responsibility, the law of international security, international humanitarian law, the law of State immunities, international trade law, human rights law and international private law.**

77. **Some unilateral sanctions in the cybersphere – preventing access to satellites, the Internet, software, publicly available information and communication platforms and services – target the entire populations of targeted countries, affecting their economic and cultural rights, including rights to the Internet, to information, to education, to health, to life and to development, as well as academic freedoms, and they constitute discrimination on the ground of nationality.**

78. **The activity of natural and legal persons in cyberspace may endanger the existence of States and may constitute a threat to international peace and security. The Charter of the United Nations does not prevent the Security Council from deciding to take enforcement measures in such conditions. The implementation of Security Council decisions today involves measures taken by States in the cybersphere.**

79. **Unilateral measures can be taken by States and regional organizations in response to malicious cyberactivity or through the use of cybermeans only in full conformity with international law, and only if the measures also do not violate any obligation in the sphere of human rights or humanitarian law, or in the course of countermeasures.**

80. **Targeted sanctions as a substitute for criminal processes in cases of cybercrimes violate economic rights, freedom of movement and due process rights. The online publication of lists of targeted individuals, offering monetary rewards while stating that the individuals committed crimes without investigations or court verdicts, affects their reputations while failing to provide for access to justice, appeal procedures, protection or redress.**

81. **In accordance with the general rules of international trade, the right of final consumers to have access to publicly offered software or cyberservices, whether**

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

free or at a charge, shall not be limited. Preventing access to specific Internet resources goes counter to the whole scope of "human rights on the Internet": access to information, freedom of expression, the right to privacy, the right to education and the right to reputation, as well as the right to decent work and other economic rights. It also violates the right to development and may result in the violation of the right to health and even of the right to life in emergency situations. It constitutes de facto discrimination against targeted societies. It also goes counter to repeated calls of the United Nations and other organizations for solidarity, cooperation and multilateralism.

82. **Despite the growing imposition of unilateral sanctions for "malicious" activities in cyberspace, legal or humanitarian assessments are usually not carried out. Consequently, matters such as freedom of expression and the permissibility of restrictions under articles 19 and 20 of the International Covenant on Civil and Political Rights, as well as assurances of due process rights, are not considered.**

83. **Any unilateral measures against activities of the media, social networks and social platforms can be carried out only if they do not violate international obligations of States, including with regard to freedom of the press, freedom of access to information and freedom of expression, and only if they comply with articles 19 and 20 of the International Covenant on Civil and Political Rights and other norms of international law to, inter alia, prohibit propaganda of war, genocide, speeches in favour of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence; to prevent the spread of child pornography; to respect the rights and reputation of other persons; or to protect State security, public order, public health or morals, subject to the criteria of good faith, reasonableness, necessity and proportionality. The burden of proving the validity of the relevant restrictions lies with the State; shifting the burden of proof to the affected media does not comply with international law.**

Recommendations

84. **Unilateral sanctions imposed with reference to malicious cyberactivity should be reviewed and lifted when they are not in conformity with Security Council sanctions or cannot be qualified as legal retorsions or countermeasures. No measures to enforce resolutions of the Security Council in the cybersphere can be taken without clear additional authorization of the Security Council.**

85. **All criteria for the attribution of activity to States, companies and individuals shall be fully observed. No sanctions can be imposed on the basis of classified intelligence information.**

86. **Unilateral sanctions shall not be used as a substitute for criminal processes regarding cybercrimes. They shall not be a substitute for the burden of proof or be used in the absence of jurisdiction. All due process and jurisdictional standards shall be observed.**

87. **States shall take measures in response to malicious cyberactivity only if there is sufficient evidence and a legal assessment has been conducted, taking into account the provisions of international law, international humanitarian law and human rights law.**

88. **Human rights shall be guaranteed to every individual around the world without discrimination. No "good intentions or objectives" can justify turning the entire population of a country into an indirect or unintended target of**

unilateral sanctions, or a target of human suffering, as "collateral damage", as this constitutes a violation of fundamental human rights.

89. **When imposing sanctions against State bodies and officials, the principle of the sovereign equality of States and the jurisdictional immunities of States and their property must be fully respected. Deviating from international legal norms and standards in the field of human rights on the basis of an administrative procedure is not allowed.**

90. **Media platforms, software development companies and businesses providing Internet services do not enjoy judicial competence and shall act in full conformity with international legal standards, exercising due diligence obligations to guarantee that their activity does not violate fundamental human rights, in particular the freedom of expression, in accordance with the Guiding Principles on Business and Human Rights.**

91. **The Security Council shall start discussions, at least at the level of the Arria formula, on the use of unilateral sanctions in response to malicious activity in cyberspace that can be considered a threat to international peace and security.**

92. **Countermeasures taken in response to malicious cyberactivity or with the use of cybermeans shall fully correspond to the requirements of the law of international responsibility: proportionality; necessity; observance of peremptory norms of international law, fundamental rights and humanitarian standards; and the prohibition of reprisals.**

93. **The Human Rights Committee shall initiate a review of its general comment No. 34 (2011) on the freedoms of opinion and expression, to guarantee that the contemporary practice of introducing unilateral sanctions, in particular limits on media, is in full conformity with the standards set out in articles 19 and 20 of the International Covenant on Civil and Political Rights, and to ensure that access to information and academic cooperation involving scholars from sanctioned countries, including the possibility to publish research, is not arbitrarily limited owing to those scholars' nationality or location.**

94. **States shall not use online platforms to target individuals suspected of crimes by disseminating unverified and therefore possibly false and defamatory information that may endanger their lives or affect their reputations, or to offer monetary rewards for information about them in connection with such information.**

95. **Any limitations on the freedom of expression online shall be taken only in full conformity with the requirements under articles 19 and 20 of the International Covenant on Civil and Political Rights. The availability of information from various sources, with the possibility of verification and comprehensive assessment, is an important means for the peaceful settlement of international disputes.**