The Changing Nature of Sanctions in the Digital Age

Alena Douhan

Abstract Cyber technologies have already changed our lives drastically. Nearly every area of social relations is currently being digitalized both nationally and internationally. The UN Security Council, in its resolutions 2419 (2018), 2462 (2019), and 2490 (2019), and many others, recognizes that the activity of individuals and non-state entities in the cyber area may constitute a threat to international peace and security. Cyber attacks on critical infrastructure; the impossibility to use online payment systems; blocking access to the Internet, Twitter and Instagram accounts, Zoom and other services; and the application of cyber measures in response to cyber threats and many others have started to be actively discussed today with regard to the problem of sanctions. This chapter seeks to provide an overview of developments and situations, when the application of sanctions is affected by the development of cyber means. It also focuses on the changes in and legal qualifications for the grounds, subjects, targets, means and methods of introduction and implementation of sanctions regimes in the digital age.

I. Introduction

The information communication infrastructure, as well as digital devices, have already become an integral part of today's reality. Digitalization has a huge impact on the development and observance of human rights, as well as on the very status of the individual. The changes are so drastic that sometimes it is even maintained that, despite the general perception of the need to apply online the same rules that are applied offline (UN General Assembly resolution A/RES/68/167 of 18 December 2013, para. 3),[1] the very notion and concept of sovereignty are outdated.[2] Individuals become all the more active in the international arena. Threats caused by the use of cyber technologies by terrorist and extremist groups had already been recognized by the UN General Assembly in 1999 (resolution 53/70 of 4

1 UNGA Res 68/167 of 18 December 2013, A/RES/68/167, para. 3.

2 Nicola Wenzel, 'Opinion and Expression, Freedom of, International Protection' in: Rüdiger Wolfrum (ed.), *MPEPIL* (online edn, Oxford: Oxford University Press 2014), available at: https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e855; Johann-Christoph Woltag, 'Cyber warfare' in: Rüdiger Wolfrum (ed.), *MPEPIL* (online edn, Oxford: Oxford University Press 2015), available at: http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e280?rskey=eCCfoY&result=7&prd=EPIL&print.

January 1999)[3] and elaborated in detail in later resolutions of the UN Security Council (resolutions 2419 (2018) of 6 June 2018,[4] 2462 (2019) of 28 March 2019[5] and 2490 (2019) of 20 September 20199.[6] The UN Security Council also mentions that young people become frequent targets of terrorist online propaganda and recruiting.[7]

Thus, it does not come as any surprise that the development of cyber means is affecting the purposes, means, mechanisms and targets of sanctions applied by the UN Security Council, regional organizations and individual states. An attack with the use of ten drones over Saudi Arabian oil extraction stations on 14 September 2019,[8] allegedly by a non-state actor from the territory of Yemen, resulted in a 60 per cent drop in oil extraction in Saudi Arabia, a 6 per cent drop in the world's oil extraction and a rise in oil prices of 15 per cent.[9] Eight individuals and four legal entities from Russia, China and North Korea have been declared to 'provide support for or [be] involved in, or facilitated cyber attacks or attempted cyber attacks publicly known as 'WannaCry' and 'NotPetya,' as well as 'Operation Cloud Hopper'.'[10]

Today, the legal scholarship pays much attention to the general aspects of cyber security,[11] the use of cyber means and methods of warfare[12] and its effects on the enjoyment of the rights to privacy and freedom

3 UNGA Res 53/70 of 4 January 1999, A/RES/53/70.
4 UNSC Res 2419 of 6 June 2018, S/RES/2419.
5 UNSC Res 2462 of 28 March 2019, S/RES/2462.
6 UNSC Res 2490 of 20 September 2019, S/RES/2490.
7 UNSC Res 2419 (n. 4), paras 9, 12.
8 'Drone attacks on Saudi oil sites disrupt supplies,' France 24 (2019), available at: https://www.france24.com/en/20190915-drone-attacks-saudi-aramco-sites-disrupt-oil-supplies-us-blames-iran.
9 Frank Gardner, 'Saudi oil facility attacks: Race on to restore supplies,' BBC (2019), available at: https://www.bbc.com/news/world-middle-east-49775849.
10 Council Implementing Regulation 2020/1125 of 30 July 2020 implementing Regulation 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States ST/9568/2020/INIT OJ L 246, 2020, 4–9.
11 Elias G Carayannis, David FJ Campbell, Marios Panagiotis Efthymiopoulos (eds), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense* (New York: Springer International Publishing 2018); Fabio Rugge, *Confronting an 'Axis of Cyber'? China, Iran, North Korea and Russia in Cyber Space* (Milano: Ledizioni 2018).
12 Woltag (n. 2); Michael Schmitt, ''Attack' as a Term of Art in International Law: The Cyber Operations Context' in: Christian Czosseck, Rain Ottis and Katharina Ziolkowski (eds), *Proceedings of the 4th International Conference on Cyber Conflict* (NATO CCD COE 2012), 287–288; Marco Roscini, 'World Wide Warfare – *Ius*

of expression,[13] the emerging right to be forgotten[14] and the violation of human rights in the digital age[15] or by being cut off from the Internet by governments.[16] Recent publications attempt to analyze specific situations relevant to the use of digital means in the course of sanctions[17] or as sanctions to limit unwelcomed online behavior.[18] However, no comprehensive overview of the impact of cyber technologies on the application and implementation of sanctions has been done in the international legal doctrine yet.

Despite the diversity of possible uses of cyber means in the modern world and the mutual impact of sanctions and the use of cyber technologies, the present article focuses on the use of cyber means as a ground for the introduction of sanctions by international and unilateral actors; blocking on-line commerce; the specifics of sanctions on trade in software; reputational risks; and blocking online educational platforms, messengers and social networks both directly and indirectly. In this regard, it is important not only to identify existing threats and challenges but to qualify them from the standpoint of international law, including for their impact on the law of human rights.

---

ad bellum and the Use of Cyber Force' in: Armin von Bogdandy and Rüdiger Wolfrum (eds), Max Planck UNYB 14 (2010), 85–130.

13 HRC, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression,' A/HRC/35/22 of 30 March 2017; UNGA, 'Report of the Special Rapporteur to the General Assembly on the Temporary Challenges to Freedom of Expression,' A/HRC/71/373 of 6 September 2016.

14 Ineta Ziemele, 'Privacy, Right to, International Protection' in: Rüdiger Wolfrum (ed.), *MPEPIL* (online edn, Oxford: Oxford University Press 2008); Janne Hagen and Olav Lysne, 'Protecting the Digitized Society: The Challenge of Balancing Surveillance and Privacy,' The Cyber Defense Review 1 (2016), 75–90.

15 Alena F. Douhan, 'Adapting the Human Rights System to the Cyber Age,' Max Planck UNYB 23 (2019), 249–289; Kai Möller 'Beyond Reasonableness: The Dignitarian Structure of Human and Constitutional Rights' CJLJ 34 (2021), 341–364.

16 Sage Cheng and Berhan Taye, 'Targeted, Cut Off, and Left in the Dark: The #KeepItOn report on internet shutdowns in 2019,' available at: https://www.accessnow.org/keepiton-2019-report.

17 Philipp Lutscher, 'Digital Retaliation? Denial-of-Service Attacks after Sanction Events' JoGSS 6 (2021), 1–11.

18 Enguerrand Marique and Yseult Marique, 'Sanctions on Digital Platforms: Balancing Proportionality in the Modern Public Square,' CLSR 36 (2020), 105372.

II. The Expanding Nature of Sanctions in International Law

The notion of sanctions is one of the most controversial ones in contemporary international law.[19] It is so often employed today in politics, criminal law, news and even everyday life and is applied to so many diverse types and categories of measures taken by entirely different subjects that neither the legality of each particular type of sanction nor its humanitarian impact are sought to be assessed anymore.

In international law, sanctions may be viewed as a power (possibility) to ensure the law,[20] an analogy of responsibility for internationally wrongful acts,[21] punishment,[22] a complex of enforcement measures (countermeasures) applied to a delinquent state,[23] a method to make someone comply,[24]

---

19 ILC, 'Articles on the Responsibility of States for Internationally Wrongful Acts with Commentaries,' (2001) ILCYB, Vol. II, Part Two, 31, 128.

20 Gerald Sparrow, *Sanctions* (London: Knightly Vernon Ltd. 1972), 11–12.

21 Aleksandr A. Kovalev and Stanislav V. Chernichenko (eds), *Mezhdunarodnoe pravo*, (3rd edn, Moscow: Prospekt 2008), 237–238 (in Russ.).

22 Ademola Abass, *Regional Organisations and the Development of Collective Security* (London: Hart Publishing 2004), 49; Ramesh Thakur, *The United Nations, Peace and Security* (Cambridge: Cambridge University Press 2010), 135. This approach is, however, disputed by the UN Secretary-General in the UN, 'Supplement to an Agenda for Peace: Position Paper,' (1995) UNGA, UNSC, A/50/60, S/1995/1 of 25 January 1995, para. 66. However, the punitive nature of sanctions has been rejected by most states: see UNSC, 'Report, 4128th Meeting,' (2000) S/PV.4128 of 17 April 2000; Johan Galtung, 'On the Effects of International Economic Sanctions' in: Miroslav Nincic and Peter Wallensteen (eds), *Dilemmas of Economic Coercion: Sanctions in World Politics* (New York: Praeger Publishers 1983), 19; Chukwudi V. Odoeme and Collins O. Chijioke, 'Sanctions in International Law: Morality and Legality at War,' CLRJ 7 (2021), 102–120 (103).

23 Gennady V. Ignatenko and Oleg I. Tiunov, *Mezhdunarodnoe pravo* (Moscow: Norma Publ. 2005), 202; Ruben Kalamkaryan and Yury Migachev, *International Law* (Moscow: Norma Publ. 2004), 182; Elena A. Shibaeva, 'International Organizations in the System of International Legal Regulation,' Soviet Yearbook of International Law 1978 (1980), 214–224 (in Russ.); Fred Grunfeld, 'The Effectiveness of United Nations Economic Sanctions' in Willem J. van Genugten and Gerard A de Groot (eds), *United Nations Sanctions: Effectiveness and Effects, Especially in the Field of Human Rights: A Multidisciplinary Approach* (Antwerp: Intersentia 1999), 115; Lori F. Damrosch, 'The Legitimacy of Economic Sanctions as Countermeasures for Wrongful Acts,' Ecology L.Q. 46 (2019), 95–110.

24 Galtung (n. 22), 19; Natalino Ronzitti, 'The Report of the High-Level Panel on Threats, Challenges and Change, the Use of Force and the Reform of the United Nations,' Italian Yearbook of International Law XIV (2004), (Leiden/Boston: Martinus Nijhoff Publishers 2005), 11.

negative consequences in the case of violation,[25] measures of protection of the international legal order,[26] measures not involving the use of armed force in order to maintain or restore international peace and security,[27] a means of implementation of international responsibility (countermeasures),[28] or measures taken by international organizations against its Member States or other actors,[29] mechanism of prompting citizens of a state to put pressure on its government.[30]

The above approaches do not specify whether they refer to universal sanctions adopted by the UN Security Council under Chapter VII of the UN Charter[31] for the maintenance of international peace and security or to unilateral measures of pressure, both military or non-military, taken without or beyond the authorization of the Security Council (unilateral sanctions). Moreover, the use of the term 'sanctions' does not automatically qualify a situation as legal or illegal.

The situation appears to be even more complicated due to the existence of other terms identifying the application of unilateral means of pressure. In particular, numerous resolutions of the UN Human Rights Council (resolutions 15/24 of 6 October 2010;[32] 19/32 of 18 April 2012;[33] 24/14 of 8 October 2013;[34] 30/2 of 12 October 2015;[35] 34/13 of 24 March 2017;[36] and

---

25 Igor I. Lukashuk, *Law of International Responsibility* (Moscow: Wolters Kluwer 2004), 309 (in Russ.); Tatiana N. Neshataeva, *International Legal Sanctions of the UN Specialized Agencies* [extended abstract of PhD dissertation] (Moscow: Moscow State University 1985), 9, 12, 14 (in Russ.).

26 Neshataeva (n. 25), 17.

27 UN, 'Supplement to an Agenda for Peace: Position Paper' (n. 22). The same approach was taken by states that participated in the discussion of the problem in the UNSC, 'UN Security Council Report oft he Agenda to the 4128th meeting,' (2000), S/PV.4128 of 17 April 2000.

28 Lukashuk (n. 25), 306, 308; The same approach is supported by Grigory I. Tunkin, Nikolai A. Ushakov, Pranas Kuris, cited by Tatiana N. Neshataeva, 'The Notion of Sanctions of International Organizations,' Jurisprudence 6 (1984), 94; Abass (n. 22), 49, 51.

29 Tom Ruys, Sanctions, Retorsions and Countermeasures: Concepts and International Legal Framework' in Larissa van den Herik (ed.), *Handbook on UN Sanctions and International Law* (Cheltenham: Edward Elgar Publishing 2017), 19–51.

30 Odoeme and Chijioke (n. 22), 105.

31 United Nations, Charter of the United Nations, 24 October 1945, 1 UNTS XVI, Chapter VII.

32 HRC Res 15/24 of 6 October 2010, A/HRC/RES/15/24, paras 1–3.

33 HRC Res 19/32 of 18 April 2012, A/HRC/RES/19/32, paras 1–3.

34 HRC Res 24/14 of 8 October 2013, A/HRC/RES/24/14, paras 1–3.

35 HRC Res 30/2 of 12 October 2015, A/HRC/RES/30/2, paras 1–2, 4.

36 HRC Res 34/13 of 24 March 2017, A/HRC/RES/34/13, paras 1–2, 4.

45/5 of 6 October 2020)[37] and the General Assembly (resolutions 69/180 of 18 December 2014;[38] 70/151 of 17 December 2015;[39] and 71/193 of 19 December 2016)[40] refer to unilateral coercive measures including but not limited to military, economic and political measures taken without or beyond the authorization of the UN Security Council, and qualify them as illegal. These resolutions, however, do not use the term sanctions. Thus, until now, there is no established distinction between sanctions, especially unilateral ones, and unilateral coercive measures.

At the same time, given the absence of a definition of unilateral coercive measures and their presumably illegal character, States prefer to present their unilateral activities as not constituting unilateral coercive measures and to use therefore other terms, like 'sanctions,' 'restrictive measures'[41] and 'unilateral measures not in accordance with international law,'[42] 'security measures,' 'countermeasures' and many others.[43] The States involved are thus also identified in various ways, including as sanctioning/sanctioned, targeting/targeted or sender/source States.[44]

It is thus possible to state that in the face of the expanded application of unilateral and multilateral measures, there is no general consent about the notion and scope of sanctions in the absence of a consensus about their application and relevant legal grounds, in the presence of multiple similar or adjunct terminology. The term 'sanctions' is used so often today without due assessment of their legality and the humanitarian impact that it starts to feel 'generally accepted.' Sanctions are presented as having a certain presumption of legality, even though they are taken in a decentralized fashion with no independent body qualifying or assessing them. The development of cyber means is affecting various aspects of the use of means of pressure.

---

37 HRC Res 45/5 of 6 October 2020, A/HRC/RES/45/5, preamble.
38 UNGA Res 69/180 of 18 December 2014, A/RES/69/180, paras 5–6.
39 UNGA Res 70/151 of 17 December 2015, A/RES/70/151, paras 5–6.
40 UNGA Res 71/193 of 19 December 2016, A/RES/71/193, paras 5–6.
41 Council of the European Union, 'Guidelines on the implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy' of 4 May 2018, doc No. 5664/18.
42 UNGA Res 70/151 (n. 31), para. 1; UNGA Res 71/193 (n. 32), para. 2.
43 HRC Res 48/59 of 25 June 2021, 'Unilateral Coercive Measures: Notion, Types and Qualification,' Report of the Special Rapporteur on the negative impact of unilateral coercive measures on the enjoyment of human rights (2021).
44 HRC, 'Report of the Special Rapporteur on the negative impact of unilateral coercive measures on the enjoyment of human rights,' (2017), A/HRC/36/44 of 26 July 2017.

The present chapter does not aim at an in-depth terminological discussion, and therefore it views sanctions as any means of pressure applied by a state or international organization, including the UN Security Council, against other states, their nationals or legal entities to change the policy or behavior of the latter without any prejudice to the legality or illegality of such activity.

III. Malicious Use of Cyber Means as a Ground for Introduction of Sanctions by International and Unilateral Actors

1. The Use of Cyber Means as a Threat to International and National Security

As mentioned above, the UN Security Council and UN General Assembly, in their resolutions,[45] have recognized that the use of new information and communication technologies even by individuals and non-State entities may constitute a threat to international peace and security.

A similar position is taken by the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, which refers to the 'dramatic increase in incidents involving the malicious use of information and communication technologies by State and non-State actors' in its report 70/174.[46] Experts uphold the opinion that the misuse of ICT (including by individuals and private entities) may harm or threaten international peace and security (para. 3).

As of the end of 2020, the UN Security Council had never imposed sanctions on states, individuals or legal entities in response to the malicious use of cyber means. It has, however, stressed that states have an obligation to control information flows, to prevent the use of the Internet for money laundering and terrorism financing, to control virtual finance and to exchange the necessary financial intelligence information[47] or aviation and passenger name data.[48] A similar call 'to prevent the use of the

45 UNSC Res 2462 (n. 5), preamble, paras 19, 21; UNSC Res 2419 (n. 4), preamble, para. 5; UNGA Res 72/246 of 24 December 2017 A/RES/72/246, paras 7–8. See also UNODC, *The Use of the Internet for Terrorist Purposes* (New York: United Nations 2012), 3–11, 32–34.

46 UNGA Res 70/174 of 22 July 2015, A/RES/70/174. 'ICT' refers to 'information and communications technology'.

47 UNSC Res 2462 (n. 5), para. 19.

48 UNSC Res 2482 of 19 July 2019, S/RES/2482, para. 15(c).

Internet to advocate, commit, incite, recruit for, fund or plan terrorist acts' has been made by the UN General Assembly.[49]

The number of people involved in terrorist activity via the Internet is enormous today. While being aware of existing skeptical approaches towards the role of the Internet in terrorism radicalization, I would join here the position of many others that large amounts of easily available violent extremist content online may have radicalizing effects in various forms.[50] Statistics show that up to 30,000 foreigners were involved in the Al Qaeda and ISIL groups by the end of 2015.[51] The UN Security Council maintains that some of the terrorist activity can be qualified not only as violating the right to life but also as war crimes, crimes against humanity or genocide.[52]

It is also generally agreed both in practice and in the legal doctrine that under certain conditions, a cyber operation may constitute an armed attack or part of an armed attack[53] or be part of a military operation in the course of a non-international military conflict.[54] As such, it may endanger the very existence of a state;[55] cause the loss of human lives (death or injury of combatants or civilians); cause the destruction or damaging of property

49 UNGA Res 73/174 of 17 December 2018, A/RES/73/174, paras 30–31.

50 Maura Conway, 'Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research,' Studies in Conflict &Terrorism 40 (2017), 77–98 (77); Ines von Behr, Anaïs Reding, Charlie Edwards and Luke Gribbon, *Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism* (online edn, Santa Monica, CA: RAND 2013).

51 UNGA, 71/384, 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism,' (2016), A/71/384 of 13 September 2016, para. 12.

52 UNSC Res 2490 (n. 6), para. 2.

53 ICRC, 'Article 2: Application of the Convention,' Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (12 August 1949) (Commentary of 2016), available at: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=BE2D518CF5DE54EAC1257F7D0036B518, paras 253–256.

54 ICRC, 'Article 3: Conflicts not of an international character,' Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (12 August 1949) (Commentary of 2016), available at: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=BE2D518CF5DE54EAC1257F7D0036B518, paras 436–437.

55 Woltag (n. 2); Yoram Dinstein, *War, Aggression and Self-Defence* (Cambridge: Cambridge University Press 2001), 175–176. Jochen A. Frowein, 'Legal Consequences for International Law Enforcement in the Case of Security Council Inaction' in: Jost Delbrück (ed.), *The Future of International Law Enforcement: New Scenarios – New Law* (Berlin: Dunker and Humblot 1993), 114–115.

(civilian or military), including critical infrastructure;[56] or cause the loss of part of a state's territory.[57] The existence of a causal link between a cyber attack and the immediacy of negative consequences can be established (seconds or minutes between the attack and its results).[58]

Special attention is also traditionally paid to so-called 'attacks on critical infrastructure' that are attacks against dams, nuclear electricity stations, arms control systems, bank accounts and operations, gas and oil pipelines, electricity lines, taxation systems, governmental servers and computer networks,[59] as well as other critical infrastructure; and the interception of control over air defense systems,[60] floodgates of dams, aircraft or trains (which can cause them to collide),[61] etc.

If such attacks meet the above criteria, they may give rise to acts of self-defense in accordance with Article 51 of the UN Charter. The above-mentioned attack accomplished with the use of ten drones over Saudi Arabian oil extraction stations on 14 September 2019[62] can serve as a good illustration that the well-being and even the very existence of states may be endangered by cyber means by a group of individuals. It appeared impossible to identify the actual perpetrators of this attack, although the UN Secretary-General, in his report to the UN Security Council S/2020/531, noted that some items subsequently seized by the United States were identified as having Iranian origin and 'were identical or similar to those found in the debris of the cruise missiles and the delta-wing uncrewed aerial vehicles used in the attacks on Saudi Arabia in 2019.'[63] In such situations, the UN Security Council will face serious problems when trying to attribute an act or acts to a specific state in order to be able to take

56 Schmitt (n. 12), 287–288; Roscini (n. 12), 106–107.

57 Pauline C. Reich, Stuart Weinstein, Charles Wild and Allan S. Cabanlong, 'Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents – and the Dilemma of Anonymity,' EJLT 1 (2010), 1–58 (26).

58 Heather Harrison, *Cyber Warfare and the Laws of War* (Cambridge: Cambridge University Press 2014), 63–73.

59 Reich et al. (n. 57), 12–17.

60 International Law Association, 'Draft Report on Aggression and the Use of Force' (May 2016), available at: https://ila.vettoreweb.com/Storage/Download.aspx?DbStorageId=1055&StorageFileGuid=c911005c-6d63-408e-bc2d-e99bfc2167e4, 18.

61 ICRC, 'Article 3: Conflicts not of an international character' (n. 54), para. 437.

62 'Drone attacks on Saudi oil sites disrupt supplies,' France 24 (2019), available at: https://www.france24.com/en/20190915-drone-attacks-saudi-aramco-sites-disrupt-oil-supplies-us-blames-iran.

63 UNSC, 'Implementation of Security Council resolution 2231(2015),' Ninth report of the Secretary-General S/2020/531 of 11 June 2020, available at: https://undocs.org/S/2020/531, paras 11–14.

appropriate sanctions towards states. It is very probable that it will have to limit itself to general recommendations or to impose targeted sanctions, for example, within the framework of sanctions against individuals and organizations involved in terrorist activity, or it may consider establishing a mixed criminal tribunal with the consent of a state concerned.

In cases when an attack on critical infrastructure does not reach the level of an armed attack but is brought in breach of international obligations or violates the rights and interests of states, the latter usually refers to the possibility to take unilateral sanctions independently or via corresponding regional international organizations. It follows from the above that cyber attacks or other offensive uses of information and communication technologies may be qualified under certain conditions as a threat to peace, a breach of the peace or an act of aggression by the UN Security Council and may thus give rise to UN sanctions against states, individuals or legal entities.

States and regional organizations also look for the framework of possible reactions to the use of the Internet for malicious activity. The Security Council in particular persistently refers to the obligation of states to 'ensure that all measures taken to counter-terrorism, including measures taken to counter the financing of terrorism as provided for in this resolution, comply with their obligations under international law, including international humanitarian law, international human rights law and international refugee law' and to 'take into account the potential effect of those measures on exclusively humanitarian activities, including medical activities, that are carried out by impartial humanitarian actors.'[64] Also, the OSCE's recommendations on countering the use of the Internet for terrorism purposes focus on domestic investigation and judicial processes.[65]

64 See UNSC Res 2462 (n. 5), paras 6, 24; UNSC Res 2482 (n. 48), preamble, para. 15(c); UNSC Res 2501 of 16 December 2019, S/RES/2501, preamble; UNSC Res 2535 of 14 July 2020, S/RES/2535, para. 7.

65 Decision 7/06 of 5 December 2006 'Countering the Use of the Internet for Terrorist Purposes,' OSCE, MC.DEC/7/06; Regional Workshop on Countering the Use of the Internet for Terrorist Purposes for Judges, Prosecutors and Investigators from South Eastern Europe of 8 February 2017, CIO.GAL/224/16, OSCE (2016), available at: https://www.osce.org/files/f/documents/7/e/299091.pdf.

2. *Overview of State Practice of Imposing Sanctions in Response to Malicious Cyber Activities*

State practice of imposing sanctions in response to real or alleged malicious cyber activities is rather extensive. In particular, United States Executive Order (EO) 13694 of 1 April 2015, as amended by later documents,[66] introduced and expanded the list of 'cyber-enabled activities subject to sanctions'[67] such as blocking property and interests in property in a broad number of cases, to include attacks on critical infrastructure, interference in the election process, disruption of networking or computer operations, misappropriation of financial funds and personal information, etc.

Some of these measures in response to malicious cyber activity are taken by the United States with reference to implementing UN Security Council resolutions against North Korea (hereafter – DPRK) in the struggle against the proliferation of weapons of mass destruction (from resolution 1718 (2006) of 14 October 2006[68] to resolution 2397 (2017) of 22 December 2017).[69] They aim to suppress attempts by North Korea to use cyber technologies to circumvent sanctions imposed both by the UN Security Council and the United States.[70]

In its Guidance on the North Korean Cyber Threat of 15 April 2020, the United States refers to disruptive or destructive cyber activities affecting critical US infrastructure: cybercrimes, espionage, cyber-enabled financial theft and money laundering, extortion campaigns and crypto-jacking. This activity may be prosecuted by the United States with a penalty of 'up to 20 years of imprisonment, fines of up to $1 million or totaling twice

66 For example, Executive Order 13757 of 28 December 2016, 'Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities,' available at: https://home.treasury.gov/system/files/126/cyber2_eo.pdf.

67 Executive Order 13694 of 1 April 2015, 'Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities,' available at: https://www.govinfo.gov/content/pkg/CFR-2016-title3-vol1/pdf/CFR-2016-title3-vol1-eo13694.pdf. See also Silvina M. Romano, 'Psychological War Reloaded: Cyber-Sanctions, Venezuela and Geopolitics,' Revista Internacional de Pensamiento Politico 12 (2017), 105–126 (113–115).

68 UNSC Res 1718 of 14 October 2006, S/RES/1718.

69 UNSC Res 2397 of 22 December 2017, S/RES/2397.

70 North Korea Committing Cybercrimes to Avoid US Sanctions (2019), available at: https://beincrypto.com/north-korea-cybercrimes-us-sanctions/; DPRK Cyber Threat Advisory, 'Guidance on the North Korean Cyber Threat,' (2019), available at: https://home.treasury.gov/system/files/126/dprk_cyber_threat_advisory_20200415.pdf.

the gross gain, whichever is greater, and forfeiture of all funds involved in such transactions' against those who violate the US sanctions laws[71] (applying secondary sanctions). The United States also offers rewards of up to 5 million US dollars for information that 'leads to the disruption of financial mechanisms of persons engaged in certain activities that support North Korea, including money laundering, sanctions evasion, cyber-crime' via the Rewards for Justice program.[72]

A Panel of Experts, established by the UN Security Council to make recommendations to the Council, Member States and the corresponding Sanctions Committee as regards the implementation of resolutions on North Korea,[73] has repeatedly noted the evasion of financial sanctions by North Korea through cyber means, including crypto-currency operations[74] and recommended the Security Council to 'consider explicitly addressing the DPRK's evasion of sanctions through cyber means if drafting additional sanctions measures' and to enhance control of the UN Member States in the sphere of cryptocurrency.[75] At the same time, no resolution of the UN Security Council authorizes any additional measures in response to DPRK cyber activity.

In this regard, it is also worth mentioning that on 21 September 2021, the United States designated SUEX OTC, S.R.O. (SUEX) as a malicious cyber actor, the first designation against a virtual currency exchange.[76] Some measures in response to serious or attempted cyber attacks, understood as actions involving access to information systems, information systems interference, data interference or data interception, have been taken by the European Union and the United Kingdom since 17 May 2019.[77] Both have

71 DPRK Cyber Threat Advisory, 'Guidance on the North Korean Cyber Threat,' (2019), available at: https://home.treasury.gov/system/files/126/dprk_cyber_threat_advisory_20200415.pdf, 8.

72 See at: https://rewardsforjustice.net/english/about-rfj/north_korea.html.

73 See UNSC Res 1874 of 12 June 2009, S/RES/1874, para. 26; and UNSC Res 2515 of 28 July 2020, S/RES/2515, para. 1.

74 UNSC, 'Report of the Panel of Experts established pursuant to resolution 1874(2009),' S/2019/691 of 29 August 2019, paras 57–71.

75 Ibid., conclusions, paras 8–11; and UNSC, 'Final report of the Panel of Experts submitted pursuant to resolution 2464 (2019),' S/2020/151 of 7 February 2020, recommendations, Annex 73, paras 26–28.

76 See 'Treasury Takes Robust Actions to Counter Ransomware,' Press Release, 21 September 2021, available at: https://home.treasury.gov/news/press-releases/jy0364.

77 Until 31 December 2020, the United Kingdom will apply the European Union cybersanctions. See at: https://assets.publishing.service.gov.uk/government/upload

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.[78]

In July 2020 and October 2020, eight individuals and four legal entities from Russia, China and North Korea were listed for being considered to have 'provided support for or were involved in, or facilitated cyber attacks or attempted cyber attacks, including the attempted cyber attack against the OPCW and the cyber attacks publicly known as 'WannaCry' and 'NotPetya,' as well as 'Operation Cloud Hopper"[79] and to have been 'involved in cyber attacks with a significant effect which constitutes an external threat to the Union or its Member States, in particular, the cyber attack against the German federal parliament (Deutscher Bundestag) which took place in April and May 2015'[80] correspondingly.

3. *Legality of Unilateral Sanctions Taken in Response to Malicious Cyber Activities*

The above practice clearly demonstrates that measures taken by states and the European Union in response to malicious cyber activities include measures aimed to enhance the internal capacity of states to suppress cyber threats as well as the application of targeted sanctions to listed individuals and companies.

The possibility to impose unilateral sanctions with the purpose of implementing relevant decisions of the UN Security Council formed a ground for extensive scholarly debate since the early 1990s. The very idea of implicit, tacit or general authorization[81] or the possibility to use

---

s/system/uploads/attachment_data/file/813212/HM_Treasury_Notice__CA_regime.pdf.

78 Council Regulation 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States OJ L 129I 2019, 1.

79 Council Implementing Regulation 2020/1125 (n. 10), 4–9.

80 Regulation 2020/1125 (n. 10), 1–4.

81 Vera Gowland-Debbas, 'The Limits of Unilateral Enforcement of Community Objectives in the Framework of UN Peace Maintenance,' EJIL 11 (2000), 373; Peter Malanczuk, *Humanitarian Intervention and the Legitimacy of the Use of Force* (The Hague: Het Spinhuis 1993), 17–19; Rein Müllerson, 'Jus ad Bellum and International Terrorism' in: Fred L. Borch and Paul S. Wilson (eds), *International Law and the War on Terror* (Newport, R.I.; Naval War College 2003), 175; Michael Byers, 'Terrorism, the Use of Force and International Law after 11 September 2001,' ICLQ 51 (2002), 401; Alexander Orakhelashvili, 'The Impact of Peremptory

enforcement measures unilaterally, when the decisions of the Security Council are not observed,[82] have been repeatedly condemned in the international legal scholarship.[83] Already in 1998, the UN General Assembly urged the international community 'to eliminate the use of unilateral coercive economic measures … which are not authorized by relevant organs of the United Nations.'[84]

Taking into account that the above measures are not authorized directly by the UN Security Council and that the UN Charter does not provide for any possibility or mechanism for states and regional organizations to take any enforcement measures unilaterally, sanctions in response to malicious cyber activity can only be legal if they do not breach any international obligation of states, including, as referred to above, obligations in the sphere of human rights; or if their wrongfulness is excluded in accordance with international law in the course of countermeasures.[85]

The above documents clearly demonstrate that sanctions are imposed by the United States, the European Union and the United Kingdom by executive bodies in the absence of court hearings or due process guarantees such as access to courts. Moreover, the reference to cyber-threats makes the acquisition and disclosure of evidence problematic and all allegations rather ill-founded. This results in the aggravation of violations that traditionally occur with targeted sanctions, in particular, of property rights, freedom of movement, the right to privacy, the right to reputation and even in some cases, labor and social rights of targeted individuals with very little possibility to protect their rights in judiciary bodies.[86]

The recent practice of the United States is rather remarkable in this regard. In June 2020, six Nigerians were listed by the Department of the Treasury's Office of Foreign Assets Control (OFAC) for stealing 'over six

---

Norms,' EJIL 16 (2005), 59–88 (63–64); Hartmut Körbs, *Die Friedensdicherung duech die Vereinten Nationen und Regionalorganizationen* (Bochum: Brockmeyer 1997), 538.

82 Rainer Hofmann, 'International Law and the Use of Military Force against Iraq,' GYIL 45 (2002), 9–34 (13–15); Edward McWhinney, 'International Law-based Responses to the September 11 International Terrorist Attacks,' Chin. J. Int. Law 1 (2002), 280–286 (282); Christian Schaller, 'Massenvernichtungswaffen und Präventivkrieg. Möglichkeiten der Rechtvertigung einer militärischen Intervention im Irak aus völkerrechtlicher Sicht,' HJIL 62 (2002), 641–668 (654).

83 See e.g. Schaller (n. 82), 654; McWhinney (n. 82), 282; Hofmann (n. 82), 13–15.

84 UNGA Res 52/181 of 4 February 1998, A/RES/52/181, para. 2.

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

86 Ibid., 98–112.

million dollars from victims across the United States' with the use of fraud involving cyber schemes.[87] 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 September 2020.[88]

While recognizing that states are under the obligation to take measures to suppress cyber crimes against the state, its nationals and legal entities, such measures shall remain within the recognized international intercourse: joining international treaties, developing legislation, starting criminal investigations and prosecutions, and judicial cooperation.[89] It is thus not clear why no criminal case has been initiated in response to the alleged cybercrimes, which would provide for the possibility to freeze assets, initiate criminal investigations, involve relevant international criminal police cooperation bodies and gather evidence. Instead, measures were taken in the form of unilateral sanctions upon the decision of the executive body, OFAC, without any identification of the beginning of criminal proceedings, any court hearing or any possibility for the listed individuals to access courts in order to protect their rights, reputations or personal data.

Moreover, the imposition of economic sanctions and entry bans, besides violating property and other rights, goes counter to the requirement of the presumption of innocence set forth in Article 14(2) of the International Covenant on Civil and Political Rights (ICCPR),[90] 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.'[91] Paragraph 30 of the General Comment No. 32 expressly notes that 'no guilt can be presumed until the charge has been proved beyond a reasonable

87 '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.

88 'Treasury Sanctions Russian Cyber Actors for Virtual Currency Theft,' Press Releases of 16 September 2020, available at: https://home.treasury.gov/news/press-releases/sm1123.

89 Decision 7/06 (n. 65); Regional Workshop on Countering the Use of the Internet for Terrorist Purposes for Judges, Prosecutors and Investigators from South Eastern Europe (n. 65).

90 UNGA, International Covenant on Civil and Political Rights, 16 December 1966, UNTS 999, 171.

91 Human Rights Committee, General Comment No. 32 of 23 August 2007, 'Article 14: Right to equality before courts and tribunals and to a fair trial,' CCPR/C/GC/32, para. 4.

doubt, ensures that the accused has the benefit of doubt' and requests governments to abstain from making public statements affirming the guilt of the accused.[92]

The Treaty on the Functioning of the European Union, unlike the US legislation, provides for the possibility to appeal to the European Court of Justice to review the legality of decisions allowing for restrictive measures against natural or legal persons adopted by the Council (Article 275[93]). The European Court of Justice has been active in the sphere of so-called 'sanctions cases,' making more than 360 judgements by December 2020.[94] No review of a cyber sanctions case has taken place until now.

Another aspect that deserves careful attention is the possibility to apply unilateral measures in response to cyber attacks and cyber threats in the course of countermeasures. In accordance with Article 49(1) of the Draft Articles on Responsibility of States for Internationally Wrongful Acts of 2001 (ARSIWA), 'An injured State may only take countermeasures against a State which is responsible for an internationally wrongful act in order to induce that State to comply with its obligations.'[95] Therefore, measures that constitute countermeasures can only be taken in response to the violation of a specific international obligation by a specific state and may be directed only against that state[96] to induce it to comply with the obligation.

Countermeasures thus can only be applied against individuals immediately responsible for the policy or activity of a state in breach of an international obligation, in order to change that policy or activity, or against states as such with due account of the attribution of the malicious cyber activity to the corresponding state (ARSIWA, Articles 4–11). Countermeasures thus are not applicable to other categories of persons or entities accused in particular of committing cybercrimes. The same approach is taken

92 Ibid., para. 30.

93 Consolidated version of the Treaty on the Functioning of the European Union OJ C 326, 2012, 47390.

94 EU sanctions. Court Judgements (2020), available at: https://www.europeansanctions.com/judgment/.

95 ILC, ARSIWA (n. 19), 43–59. See also Institut de Droit International, 'The Protection of Human Rights and the Principle of Non-Intervention in Internal Affairs of States,' Session in Santiago de Compostela (1989), available at: https://www.idi-iil.org/app/uploads/2017/06/1989_comp_03_en.pdf.

96 In support, see Dorothee Geyrhalter, *Friedenssicherung durch Regionalorganisationen ohne Beschluß des Sicherheitsrates* (Cologne: LIT 2001), 66.

by the drafters of Tallinn manual 2.0 on the international law applicable to cyber operations (Rules 20–21).[97]

In this regard, a provision of Article 1(6) of Council Regulation (EU) 2019/796 of 17 May 2019 does not fit the requirement of Article 49(1) of ARSIWA as it speaks about the possibility to impose sanctions 'where deemed necessary to achieve common foreign and security policy (CFSP) objectives' rather than in response to an internationally wrongful act. Moreover, the possibility to apply restrictive measures 'in response to cyber attacks with a significant effect against third States or international organisations' rather than the EU or its Member States provides for the possibility of any action in the course of countermeasures only if underlying violations have a so-called collective nature in accordance with Article 48 ARSIWA.

Another aspect which comes into discussion of the possibility to apply unilateral sanctions as countermeasures is the difficulty of attributing the activity of specific individuals or other non-state entities to a specific state for the purposes of holding it responsible, as shown above in the case of the cyber attack against Saudi oil installations. The traditional approach refers to the need for 'effective'[98] or 'overall'[99] control from the side of the specific state. I would align myself here with the position of the drafters of the Tallinn manual 2.0 that the same rules of attribution of activity of non-state actors to states (acting under direction and control) shall be applied to the activity in the cybersphere as international law does not provide any additional or different regulation.[100]

Therefore, unilateral sanctions against allegedly malicious cyber activity can only be taken if they do not violate any obligation of a state, including in the sphere of human rights (retortion) or as countermeasures in full compliance with international law in accordance with basic principles of the law of international responsibility, with the purpose to restore the observance of international obligations, prior notice, and observance of the rule of law, including legality, legitimacy, humanity and proportionality to

97 Michael N. Schmitt (ed), *Tallinn manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge: Cambridge University Press 2017), 111- 122.

98 ICJ, *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America), merits, judgment of 27 June 1986, ICJ Reports 1986, 14, (paras 113–115).

99 ICTY, Appeals Chamber, *The Prosecutor v. Dusko Tadić*, 15 July 1999 (case no. IT-94–1-A), paras 120–124, 146.

100 Tallinn manual 2.0 (n. 97), 94–96.

the harm suffered (ARSIWA, Articles 49–51),[101] with due account for the precautionary approach as concerns the humanitarian impact of measures taken. Under Article 50(1)(b) ARSIWA, the obligations for the protection of fundamental human rights can never be affected by countermeasures. As correctly noted by Alexander Kern, punitive sanctions have mostly been geared towards the past,[102] and in the contemporary world, shall be taken in accordance with international law standards.

IV. Blocking On-line Commerce

The blocking of online commerce has turned into one of the frequently used forms of unilateral sanctions today – a means of implementation of economic and financial sanctions, as far as international transactions are mostly happening online. Today, blocking online payments constitutes an integral part of the implementation of UN Security Council sanctions[103] and of the Financial Action Task Force (FATF) recommendations aimed to suppress money laundering and terrorism financing.[104] Today funds and assets are understood by the FATF to include also those existing in electronic and digital form.[105] Further, recommendation 16 of the FATF imposes on financial institutions obligations aimed to facilitate 'identification and reporting of suspicious transactions and to implement the requirements to take freezing action and comply with prohibitions from conducting transactions with designated persons and entities'[106] *inter alia* via virtual means.

The impossibility to make financial transfers to/from targets of sanctions has been cited *inter alia* as a part of trade and financial sanctions

---

101 Even so, Geyrhalter, for example, claims it is possible that economic sanctions may be applied to states responsible for mass violations of fundamental human rights; see Geyrhalter (n. 96), 66; ILC, ARSIWA (n. 19), para. 6. See also Antonios Tzanakopoulos, 'State Responsibility for Targeted Sanctions,' AJIL 113 (2019), 135–139 (136–137).

102 Alexander Kern, *Economic Sanctions: Law and Public Policy* (New York: Palgrave Macmillan 2009), 62.

103 UNSC Res 1874 (n. 73), paras 18–19; UNSC Res 2462 (n. 5), paras 2–4.

104 Recommendation 36 FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation,' adopted by the FATF plenary in February 2012 (Updated October 2021), available at: www.fatf-gafi.org/recommendations.html, 27.

105 Ibid., 124, 130.

106 Ibid., 78.

as concerns transactions with Cuba,[107] Iran, Venezuela, Syria and other states.[108] In particular, any transactions, including online transactions made by US persons (individuals and legal entities) or made in or involving the United States relating to the property or interests in property of sanctioned individuals, are prohibited unless authorized or exempted.[109]

The situation is aggravated by the fact that the majority of the elements that enable any individual, corporation or government to trade are concentrated either within the United States or the European Union. This jurisdiction provides the United States in particular with the possibility to control and block all payments in US dollars via Visa, MasterCard, American Express, Western Union and PayPal.[110] Another illustrative example could be seen in the repeated calls to cut off SWIFT – the information exchange system connecting more than 11,000 financial institutions from 200 countries and territories –[111] as part of sanctions against Iran, Israel, the Russian Federation Belarus and China.[112] On the other hand, using SWIFT to block transactions as a countermeasure to the US sanctions has also been considered within the EU.[113]

---

107 Luis Rondon Paz, 'The External Blockade and Internet Sanctions on Cuba,' Havana Times (2015), available at: https://havanatimes.org/opinion/the-external-blockade-and-internet-sanctions-on-cuba/.

108 Statements of states during the Virtual Arria meeting of the UN Security Council of 25 November 2020 (2020), available at: http://webtv.un.org/live/watch/part-12-virtual-arria-meeting-on-%E2%80%9Cend-unilateral-coercive-measures-now%E2%80%9D/6212373519001/?term=. See also Call for submissions: UCM-Study on impact of unilateral sanctions on human rights during the state of emergency amid COVID-19 pandemic (2020), available at https://www.ohchr.org/EN/Issues/UCM/Pages/call-covid.aspx.

109 United States, Cyber-Related Sanctions Program, available at: www.treasury.gov/resourcecenter/sanctions/
Programs/Documents/cyber.pdf.

110 See Renata Avila Pinto, 'Digital Sovereignty or Digital Colonialsim,' Sur – International Journal on Human Rights 27 (2018), 15–28 (20).

111 SWIFT. About us (2020), available at: https://www.swift.com/about-us.

112 Brian O'Toole, 'Don't believe the SWIFT China sanctions hype,' Atlantic Council (2020), available at: https://www.atlanticcouncil.org/blogs/new-atlanticist/dont-believe-the-swift-china-sanctions-hype/; 'SWIFT Says It 'Has No Authority' To Unplug Russia Or Israel,' PYMNT (2014), available at: https://www.pymnts.com/in-depth/2014/swift-says-it-has-no-authority-to-unplug-russia-or-israel/; 'Economist: Disconnecting from SWIFT Will Be a Bomb for the Regime' (2020), available at: https://charter97.org/en/news/2020/11/25/401835/.

113 Tobias Stoll, 'Extraterritorial sanctions on trade and investments and European responses Policy Department for External Relations,' Directorate General for External Policies of the Union PE 653.618 (2020), available at: https://www.europa

It has been generally recognized in economic and legal scholarship that a limited number of service providers, as well as the interdependence or dependence on a specific resource (financial system, currency, etc.), results in a special vulnerability of both non-controlling countries and the end-users,[114] while digital platforms may be used not only for transactions but for many other purposes.[115] In the contemporary interdependent world, being disconnected from the single bank payment system would have not a targeted but rather a comprehensive impact, affecting the country as a whole, every single individual and company on its territory, as well as every third-country national and company involved in economic transactions with the latter, resulting in an economic crisis. That is why Russia, China and India not only developed national payment systems but are exploring the possibility to establish an alternative to SWIFT.[116]

Other types of blocking online commerce through the implementation of sectoral or targeted sanctions generally result in the extension of the time necessary to complete transactions, increasing bank costs and entrepreneurial risks, the shutting down of investments and the impossibility to buy or order even essential goods, including medicine, medical equipment, food, electricity, etc.[117] This badly affects a number of fundamental human rights, including the right to health, the right to food and economic rights; it gives rise to poverty and, in some cases, may result in the violation of the right to life.

Additional sanctions imposed by the United States on 18 Iranian banks on 8 October 2020 prevent any possibility for online transactions involving

---

rl.europa.eu/thinktank/en/document.html?reference=EXPO_STU(2020)653618, 12.

114 Allan E. Gotlieb, 'Extraterritoriality: A Canadian Perspective,' Nw. J. Int'l L. 5 (1983), 449 (451).

115 Marique and Marique (n. 18), 5.

116 Dipanjan Roy Chaudhury, 'India-Russia-China explore alternative to SWIFT payment mechanism,' The Economic Times (2019), available at: https://economictimes.indiatimes.com/news/economy/foreign-trade/india-russia-china-explore-alternative-to-swift-payment-mechanism/articleshow/72048472.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.

117 UNGA, 'Negative impact of unilateral coercive measures on the enjoyment of human rights in the coronavirus disease pandemic,' Report of the Special Rapporteur on the negative impact of unilateral coercive measures on the enjoyment of human rights, Alena Douhan. A/75/209 of 21 July 2020, available at: https://www.undocs.org/en/A/75/209; Joint Communiqué, 'Unilateral Coercive Measures (UCMs) and their Impacts in the Context of COVID-19,' Vienna, 30 November 2020, available at: https://viennaun.mfa.ir/en/newsview/619102/Joint-Communiqu%C3%A9-on-UCMs-and-their-Impacts.

US dollars. EU officials thus express concerns that it will close off any possibility for Iran to use 'foreign currency for humanitarian imports,' in particular medicine and grains.[118] The most urgent problems involve the impossibility to buy European medicines, including insulin necessary for the survival and well-being of millions of diabetics in the country.[119] Humanitarian organizations working in the targeted countries unanimously refer to the impossibility to make bank transfers to and from these states for the supply and delivery of essential goods.[120] Private companies and individuals from Venezuela, Syria, Cuba and other countries under sanctions refer to the impossibility to open or keep bank accounts or to do transactions because of their nationality also when they are not included in the lists.[121]

It is often maintained that the problem of blocking accounts is exacerbated by the extraterritorial application of sanctions[122] and over-compliance. Due to the high risks of applying criminal and civil penalties even for transactions taking place outside the US or the European Union, banks are reluctant to permit bank transfers or significantly extend transfer terms, and other companies are unwilling to be involved in transactions because of the fear of secondary sanctions, even when companies in targeted countries are not included in sanctions lists.[123] In particular, private and public sector banks in Switzerland have suspended money transfers to Cuba, preventing some Swiss humanitarian organizations from collaborating

118 John Hudson, 'Trump administration imposes crushing sanctions on Iran in defiance of European humanitarian concerns,' The Washington Post (2020), available at: https://www.washingtonpost.com/national-security/trump-administration-to-impose-crushing-sanctions-on-iran-in-defiance-of-european-humanitarian-concerns/2020/10/07/f29c052c-08f4-11eb-991c-be6ead8c4018_story.html.

119 Rohollah Faghihi, 'Millions of Iranians at risk as US sanctions choke insulin supplies,' Middle East Eye (2020), available at: https://www.middleeasteye.net/news/iran-insulin-medicine-us-sanctions-millions-risk.

120 Speech of the representative of the Syria Red Crescent at the Virtual Arria Meeting 25 November 2020 (2020), available at: http://webtv.un.org/live/watch/part-12-virtual-arria-meeting-on-%E2%80%9Cend-unilateral-coercive-measures-now%E2%80%9D/6212373519001/?term=.

121 See Preliminary findings of the visit to the Bolivarian Republic of Venezuela by the Special Rapporteur on the negative impact of unilateral coercive measures on the enjoyment of human rights, available at: https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=26747&LangID=E.

122 Tzanakopoulos (n. 101), 139. The same opinion has been expressed by humanitarian NGOs at the Expert concultations on 21–22 October 2020.

123 Alan Boyle, 'Extra-territoriality and U.S. economic sanctions,' International Enforcement Law Reporter 36 (2020), 101–103.

with Cuban medical entities.[124] The illegality of this approach is cited *inter alia* in the study prepared upon the request of the INTA Committee, demonstrating its danger even for huge economies like that of the European Union.[125]

It has been repeatedly reported by states and humanitarian organizations that delays and the increasing costs of bank transfers and deliveries result in rising prices for medical equipment, food and other essential goods, notably in the Bolivarian Republic of Venezuela, Sudan, Syria, Iran and other countries.[126] Venezuela, in particular, refers to the fact that the duration of bank transfers from or to the country increased from 2 to 45 days, as bank fees rose from 0.5 per cent to 10 per cent.[127]

The complexity, comprehensiveness and extraterritoriality of legislation have resulted in the establishment of workarounds. One such workaround welcomed by the UN Special Rapporteur on the negative impact of unilateral coercive measures on the enjoyment of human rights is the Instrument in Support of Trade Exchanges (INSTEX), which was created in 2019 by France, Germany and the United Kingdom to foster trade between Eu-

124 CETIM, 'Economic sanctions and COVID-19 pandemic,' (2020) Europe -Third World Centre.

125 Stoll (n. 113), 18–19, 26–27.

126 Submission by the Coalition of Sudanese Doctors Abroad for SR UCM-Study on the impact of unilateral sanctions on human rights during the state of emergency in the context of COVID-19 pandemic of 15 June 2020 (2020), available at: https://www.ohchr.org/Documents/Issues/UCM/submissions/privates/SudaneseDoctorsAbroad.docx; Joint Submission by Center for Economic and Policy Research, Charity and Security Network, and American Friends Service Committee of 15 June 2020 (2020), available at: https://charityandsecurity.org/wp-content/uploads/2020/07/Joint-Comments-UNSR-Coercive-Measures.pdf; Note 100/20 of the Permanent mission of Syrian Arab Republic to the United Nations Office and Other Organizations in Geneva of 15 June 2020 (2020), available at: https://www.ohchr.org/Documents/Issues/UCM/submissions/states/Syria.doc; Note 252/2020 of the Permanent Mission of Cuba to the United Nations Office in Geneva and the International Organizations in Switzerland of 04 May 2020 (2020), available at: https://www.ohchr.org/Documents/Issues/UCM/submissions/states/CUBA.docx; Syria Red Crescent statements, 'End Unilateral Coercive Measures Now,' Virtual Arria meeting of 25 November 2020 (2020), available at: https://www.securitycouncilreport.org/whatsinblue/2020/11/arria-formula-meeting-on-unilateral-coercive-measures.php.

127 Note Verbale 0116 of 29 May 2020, 'Input of the Bolivarian Republic of Venezuela for the study regarding the impact of unilateral sanctions on human rights during the state of emergency in the context of COVID-19 pandemic' (2020), available at: https://www.ohchr.org/Documents/Issues/UCM/submissions/states/Venezuelapart1.docx.

rope and the Islamic Republic of Iran and to protect European businesses by circumventing United States sanctions against that country. The initial transactions involved humanitarian goods used by the Islamic Republic of Iran to fight COVID-19.[128]

Cyber-technologies are also influencing the scope of private entities involved in the implementation of sanctions regimes. In particular, the United States Cyber-Related Sanctions Regulations impose special obligations on US persons facilitating or engaging in online commerce.[129] The EU regulations request that 'natural and legal persons, entities and bodies supply immediately any information which would facilitate compliance with this Regulation…'[130] Humanitarian organizations repeatedly refer both to the impossibility to make money transfers or to buy essential goods to be delivered to targeted states and to their fear of being subjected to secondary sanctions because of their humanitarian activity.

Nothing in international law can be interpreted to permit any impediment of bank transfers without authorization of the UN Security Council or outside of criminal procedures under national legislation. Even in situations when countermeasures can be taken in response to violations of international law, they are to be taken in accordance with the principles of proportionality and necessity and in compliance with human rights and humanitarian obligations. The fear of secondary sanctions by banks and private companies results in over-compliance and non-selectivity in the sphere of online commerce, making it impossible for nationals of listed countries to enjoy their rights and limiting their access to humanitarian aid.

V. Sanctions on Trade in and Access to Software

1. Overview

The software can also be qualified as a commodity today. As a result, trade in software can also be limited as part of a sanctions regime. In

128 'EU sells medical goods via INSTEX,' Financial Tribune, (2020), available at: https://financialtribune.com/articles/business-and-markets/102669/eu-sells-medical-goods-via-instex; Stoll (n. 113), 75.

129 Executive Order 13694, section 1a; Executive Order 13757.

130 Art. 8, Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

particular, already by 2010 the EU had imposed restrictions on the transfer of software, notably those with dual – military and civilian – use.[131]

It shall also be noted that the EU regulations provide for substantial lists of exemptions. In particular, restrictions are not expanded to software that is in the public domain, 'designed for installation by the user without further substantial support by the supplier and which is generally available to the public by being sold from stock at retail selling points.'[132]

The US approach differs substantially. Today the United States has expanded the list of restrictions on the trade of software to 'technology, and software relating to materials processing, electronics, telecommunications, information security, sensors and lasers, and propulsion, including traditional encryption and geospatial software.'[133] It thus causes the companies developing software under US jurisdiction to be concerned about complying with sanctions regimes regarding trade in software provided through public offer, used for private purposes and sometimes even at no cost,[134] to a number of countries, including (as of 2017) the Balkan countries, Belarus, Burma, Cote d'Ivoire (Ivory Coast), Cuba, the Democratic Republic of the Congo, Iran, Iraq, Lebanon, Libya, North Korea, Somalia, Sudan, Syria, and Zimbabwe;[135] and also to become extremely concerned about the growing level of software piracy.[136] As a result, because of the imposed

131 Common Military List of the European Union, ST/5470/2020/INIT of 17 February 2020, OJ C 85, 2020, 1–37, ML 21; Council Regulation 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items OJ L 134, 2009, p. 1–269, Art. 1(2); Council Regulation 267/2012 of 23 March 2012 concerning restrictive measures against Iran and repealing Regulation 961/2010 *OJ L 88, 2012, 1–112, Art. 2(2);* Council Regulation 2016/44 of 18 January 2016 concerning restrictive measures in view of the situation in Libya and repealing Regulation 204/2011 OJ L 12, 2016, 1–26, Annex I, para. 6; Council Regulation 401/2013 of 2 May 2013 concerning restrictive measures in respect of Myanmar/Burma and repealing Regulation 194/2008 OJ L 121, 2013, 1, Art. 3b, c.

132 Council Regulation (EC) No 428/2009 of 5 May 2009, Annex I; Council Regulation (EU) No 401/2013 of 2 May 2013, Annex III.

133 Gibsonn Dunn, 'Mid-year sanctions and export controls update' (2020), available at: https://www.gibsondunn.com/wp-content/uploads/2020/08/2020-mid-year-sanctions-and-export-controls-update.pdf.

134 Tyler Fuller, 'Global software collaboration in the face of sanctions,' The GitHub Blog (2019), available at: https://github.blog/2019-09-12-global-software-collaboration-in-the-face-of-sanctions/.

135 Ted Miracco, 'The Importance of Export Compliance for Software Companies,' Cylynt Blog (2017), available at: https://www.cylynt.com/blog/the-importance-of-export-compliance-for-software-companies.

136 Ibid.

prohibition on the export of technology, Syria appears to have been unable to buy software for CT scanners and ventilators that is produced only by US companies[137] and is vital in the course of the COVID-19 pandemic.

Because of the fear of secondary sanctions, companies under US jurisdiction have to comply with limitations concerning the software traditionally used for regular administration, public and private purposes, in particular for commercial Internet services or connectivity[138] and even for non-commercial activity. This has become especially dangerous in the course of COVID-19. In particular, the terms of service for Zoom as of 20 August 2020 precluded the use of the platform by those living in the DRPK, Iran, Syria and Crimea, or through legislation of the United States,[139] even for contacts and coordination among doctors to exchange their experiences on symptoms, diagnostics and means of treatment.

Limitations on the use of Zoom for official purposes appeared to be even greater. Because of the above reasons, it was not possible to use Zoom for UN communications as initially planned. Cuba, in particular, was unable to participate in a virtual summit meeting on Zoom of leaders of the Organization of African, Caribbean and the Pacific States on 3 June 2020 to discuss the COVID-19 pandemic.[140] Some countries (in particular, Belarus) have negotiated access permission on a bilateral basis. As a result, the UN Secretariat has had to invest in the development of a special UN platform.[141] It has been reported that Iranian citizens cannot get access to information on COVID-19 and its symptoms, even from the Iranian government, due to Google's censoring of AC19, an Iran-developed App.[142]

---

137 Note 100/20 of the Permanent mission of Syrian Arab Republic (n. 126).

138 Executive Order 13685 of 19 December 2014 blocking property of certain persons and prohibiting certain transactions with respect to the Crimea region of Ukraine: General License No. 9 – exportation of certain services and software incident to Internet-based communications authorized, available at: https://www.federalregister.gov/documents/2014/12/24/2014-30323/blocking-property-of-certain-persons-and-prohibiting-certain-transactions-with-respect-to-the-crimea, para. (d).

139 Zoom terms of service (2020), available at: https://zoom.us/terms.

140 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,' Granma (2020), available at: http://www.granma.cu/hilo-directo/2020-06-05/hilo-05-06-2020-00-06-14.

141 Note of the Permanent Mission of the Republic of Belarus to the United Nations Office and Other Organizations in Geneva 02–16/721 of 17 June 2020.

142 Responses and Comments from the Islamic Republic of Iran of 15 June 2020 (2020), available at: https://www.ohchr.org/Documents/Issues/UCM/submissions/states/Iran.docx.

Iranian doctors cannot get access to medical databases (Pub Med) after its server had been transferred to Google.[143]

2. *Human Rights Impact*

Therefore, impediments to accessing publicly offered platforms result in the violation of the rights of access to information and freedom of communication and the right to health. Violations of the right to education have also been cited in Iran, Sudan and Venezuela because of the impossibility of using online platforms for educational purposes. In the longer term, with a view to the deteriorating economic situation, OHCHR Sudan reported that unilateral sanctions in the course of COVID-19 are very probably affecting school enrolment and increasing the school dropout rate.[144]

The same problems remain no less relevant outside of the COVID-19 context. Access to Internet technologies and Internet resources have been referred to as a necessary element not only of the struggle against the pandemic but also of the right to development by the participants of the 'Global-local interlinkages I: Obstacles to realizing the right to development and to addressing poverty and inequality' panel of the UN Social Forum 2020.[145] The same approach is taken by the UN Human Rights Council[146] and by the Special Rapporteur on the freedom of opinion.[147]

---

143 Ibid.

144 Submission by the Coalition of Sudanese Doctors Abroad for SR UCM-Study on the impact of unilateral sanctions on human rights during the state of emergency in the context of COVID-19 pandemic of 15 June 2020, available at: https://www.ohchr.org/Documents/Issues/UCM/submissions/privates/SudaneseDoctorsAbroad.docx.

145 UN Social Forum on 8 October 2020 (2020), available at: http://webtv.un.org/watch/2nd-meeting-social-forum-2020-/6199054565001/?lan=russian#player.

146 HRC Res 32/13, 'The promotion, protection and enjoyment of human rights on the Internet,' A/HRC/32/L.20 of 27 June 2016, available at: https://documents-dds-ny.un.org/doc/UNDOC/LTD/G16/131/89/PDF/G1613189.pdf?OpenElement, preamble.

147 UNGA, 'Promotion and protection of the right to freedom of opinion and expression,' Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 66/290 of 10 August 2011, available at: https://www.ohchr.org/documents/issues/opinion/a.66.290.pdf, paras 45–75.

The OSCE Declaration on Freedom of Communication on the Internet of 28 May 2003 thus 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).[148]

The Declaration of Principles 'Building the Information Society: a global challenge in the new Millennium' of 12 December 2003 calls for states to ensure for all access to information and communication infrastructure and technologies, information and knowledge (paras. 19–28)[149] and considers information and communication technology as the means to promote the Millennium Development Goals (paras. 1, 2). The report of the ILO Global Commission 'Work for a Brighter Future' of January 2019 speaks about using technology as the means of advancing education and decent work.[150]

The UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance correctly noted in her report to the Human Rights Council in June 2020 that people from the least developed countries have only one-fourth of the opportunity to access the Internet compared to people in other countries because of poverty and the underdevelopment of the cyberinfrastructure that results in the limitation of access to 'public health information online and to make use of digital schooling, working and shopping platforms' which are especially important in the time of COVID-19 (Report A/HRC/44/57 of 18 June 2020, para. 20[151]).

It is thus believed here that one should not speak about the possibility to choose trade partners when one speaks about publicly offered paid or non-paid cyber software or services. Preventing people in targeted countries to have access to these services violates a number of human rights, including access to information, freedom of communication, the right to

148 OSCE Declaration of 28 May 2003, 'Declaration on freedom of communication on the Internet,' OSCE (2003), available at: https://www.osce.org/fom/31507?download=true. Principle 4.

149 Declaration of Principles. Building the Information Society: a global challenge in the new Millennium of 12 December 2003, WSIS-03/GENEVA/DOC/4-E (2003), available at: https://www.itu.int/net/wsis/docs/Geneva/official/dop.html.

150 ILO, 'Work for a Brighter Future,' ILO Global Commission of January 2019, available at: https://www.ilo.org/wcmsp5/groups/public/---dgreports/---cabinet/documents/publication/wcms_662410.pdf, paras 43–44.

151 UNGA, 'Racial discrimination and emerging digital technologies: a human rights analysis,' Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, A/HRC/44/57 of 18 June 2020, available at: https://undocs.org/en/A/HRC/44/57, para. 20.

education, the right to decent work and other economic rights, the right to health, the right to development and even the right to life; and it also constitutes *de facto* discrimination against targeted societies constituting around 20 per cent of the world population.

VI. Other Aspects of Application of Sanctions in the Digital Sphere

A number of other aspects of international law are affected by the development of sanctions in the digital age. One of them is the expanding practice of blocking social media accounts as part of sanctions regimes, as is done in particular by US-registered companies as part of the Magnitsky sanctions regime.[152] It has been repeatedly reported that cyber censorship takes place overall to prevent the distribution of information that may be considered harmful for the government for one or another purpose.[153] While recognizing that states are obliged to control the content of *inter alia* social media to prevent the commission of cybercrimes, involvement in terrorist activity as requested by the UN Security Council (see above) and other illegal activity, it shall be done only if international and national human rights standards are fully observed.

Access to the Internet and access to information can also be prevented by sanctions indirectly. In particular, Venezuela refers to the impediment to the access to information via television due to the cessation of operation of DirecTV Venezuela, which represented 43 per cent of the market, because of the US sanctions, in May 2020.[154] Shortages of fuel in the country also result in electricity shutdowns that make access to the Internet quite often impossible.

The availability of information via online news and press releases of state organs increases reputational risks affecting *inter alia* the right to reputation. The UN Human Rights Committee, in General Comment No. 16, refers to the obligation of states not only not to infringe the honour and reputation of individuals but also to provide adequate legisla-

152 Donie O'Sullivan and Artemis Moshtaghian, 'Instagram says it's removing posts supporting Soleimani to comply with US sanctions,' CNN Business (2020), available at: https://edition.cnn.com/2020/01/10/tech/instagram-iran-soleimani-posts/index.html; Jonny Tickle, 'Chechen leader Kadyrov banned from Instagram again, loses account with 1.4 million followers,' RT (2020), available at: https://www.rt.com/russia/488533-kadyrov-banned-instagram-again/.

153 See Avila Pinto (n. 110), 19.

154 Note Verbale 0116 (n. 127).

tion to guarantee their protection.[155] Moreover, General Comment No. 32 expressly notes that 'no guilt can be presumed until the charge has been proved beyond a reasonable doubt, ensures that the accused has the benefit of doubt' and requests governments to abstain from making public statements affirming the guilt of the accused.[156] 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 counter-parts, resulting in over-compliance with sanctions regimes. The problem becomes especially sensitive when one speaks about individuals and companies designated by one or several countries when there is no possibility for either judicial protection or redress.

The situation is exacerbated by the fact that quite often, targeted individuals and entities usually are not informed in an official and direct manner about their listing, the nature and cause of the accusation giving rise to the sanctions, the scope of limitations, the possibility to defend oneself and to have adequate time to prepare one's defense, and to have an effective remedy. Electronic databases of sanctioning states and international organizations are usually rather complicated and confusing, making the fact of sanctioning rather non-transparent. Unfortunately, the scope of individuals and legal entities targeted by such sanctions is expanding without any attempt to fill these gaps.

Promising rewards for locating individuals allegedly involved in terrorist activity without any case being started against them, and quite often without information being properly verified, on the Rewards for Justice official webpage or its Twitter account[157] is not only ruining their reputation but may endanger their life.

Some other authors refer to the use of online resources and to the element of so-called 'shaming campaign' in the course of the use of unilateral sanctions as a means, which increase reputational risks of states.[158] Social media are often used as an element of sanctions' advocacy tool by various

155 Human Rights Committee, General Comment No. 16 of 8 April 1988, 'Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation,' CCPR/C/GC/16, para. 11.

156 HRC General Comment No. 32 (n. 91), para. 30.

157 UA USA 9/2021 of 2 February 2021, available at: https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=25985.

158 Odoeme and Chijioke (n. 22), 106–107.

interlocutors.[159] Ph.M. Lutscher seeks to assess the use of DoS attacks by targeted states as a retaliation to the sanctions imposed.[160] All the above situations have not been assessed from the point of international law quite often because of the insufficiency or unavailability of data.

Quite often, countries facing serious economic sanctions, including freezing assets and blocking online commerce, start to develop their own crypto-currency (e.g. attempts done by Venezuela and North Korea). The world is currently facing the recent practice of imposing US sanctions for transactions with the use of these crypto-currencies regardless of the agents or banks in these transactions.[161]

Using cyber means and equipment as a part of sanctions policy and national sanctions acts have also been discussed in the legal scholarship. It is possible to cite here, in particular, cyber-espionage and cyber-surveillance.[162] The UN Special Rapporteur on terrorism and human rights, in his Report 34/61 of 21 February 2017, criticizes the emerging practice of using drones for targeted killings (lethal attacks) of terrorist leaders.[163] I align myself here with his opinion that this activity constitutes a clear violation of the right to life of the targeted person as well as people who may happen to be nearby; no procedural guarantees are observed (Article 14 ICCPR), and the presumption of innocence (Article 14(2) ICCPR) is also violated.[164] In practice, the use of drones for targeted killings in the considered situation could be qualified as the death penalty exercised without any guarantees, which is a clear violation of international legal standards even as regards international crimes, including war crimes (com-

159 Preliminary findings of the visit to the Republic of Zimbabwe by the Special Rapporteur on the negative impact of unilateral coercive measures on the enjoyment of human rights of 28 October 2021, available at: https://www.ohchr.org/Documents/Issues/UCM/Statements/Zimbabwe-country-visit_preliminary-observations-conclusions-Oct2021.docx.

160 Lutscher (n. 17).

161 U.S. Sanctions Venezuela's 'Petro' Cryptocurrency Amid Broader Trend of Sanctioned and Rogue Regimes Experimenting with Digital Assets, Cleary Gottlieb (2018), available at: https://www.clearytradewatch.com/2018/04/u-s-sanctions-venezuelas-petro-cryptocurrency-amid-broader-trend-sanctioned-rogue-regimes-experimenting-digital-assets/.

162 Romano (n. 67), 113.

163 HRC, 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism,' A/HRC/34/61 of 21 February 2017, available at: https://www.ohchr.org/documents/issues/terrorism/a-hrc-34-61.pdf.

164 See also HRC Res 27/37 of 30 June 2014, A/RES/27/37, para. 14.

mon Article 3 of all Geneva Conventions 1949; Article 75(4) Additional protocol I).

VII. Conclusions

The development of digital technologies has changed and is still changing all aspects of human life and international law, including the scope, subjects, means and methods of international and unilateral sanctions. The following list provides some examples but is not exhaustive: response to armed attacks and threats to international peace and security; use of cyber means for terrorism financing; malicious cyber activity, including attacks on critical infrastructure not reaching the level of an armed attack; blocking online commerce of targeted states, companies and individuals as well as other nationals; preventing access to public online platforms; blocking trade with software or information-communication equipment; blocking social media accounts; listing of crypto-currencies; and many others.

The activity of natural and legal persons in cyberspace may endanger the existence of states and constitute a threat to international peace and security. The Charter of the United Nations does not prevent the UN Security Council from deciding to take enforcement measures in such conditions, in accordance with Chapter VII of the Charter. Until now, however, the Security Council has not taken any action in response to malicious cyber activity.

The implementation of Security Council decisions and FATF recommendations today involves measures taken by states in the cybersphere, including data surveillance and the blocking of terrorist and extremist sites, online schemes of transboundary crimes, terrorist recruiting, financing and money laundering. At the same time, no measures to enforce resolutions of the UN Security Council in the cybersphere can be taken without clear additional authorization of the Security Council. National mechanisms shall, in the first place, involve organizational, legislative and judicial means taken in accordance with international law, FATF and OSCE standards.

Unilateral measures can be taken by states and regional organizations in response to malicious cyber activity or with the use of cyber means only in full conformity with international law, and if they also do not violate any obligation of the corresponding states in the sphere of human rights or humanitarian law or in the course of countermeasures. The latter measures shall fully correspond to requirements of the law of international

responsibility: proportionality, necessity, observance of peremptory norms of international law, fundamental rights and humanitarian standards, and prohibition of reprisals.

Criminal responsibility for the malicious cyber activity shall in no way be substituted by the application of unilateral sanctions. The application of targeted sanctions in such cases violates economic rights, freedom of movement, the presumption of innocence, due process standards, the right to judicial protection and the right to reputation. Public online announcements of lists of targeted individuals affect their reputations while not providing for access to justice, appeal procedures, protection or redress. Therefore, issues arising from the traditional application of targeted sanctions are equally relevant to the cyber area.

The increasing number of unilateral sanctions, with sanctions regimes that are not always transparent or for which information is not easily available results in growing over-compliance on the part of banks and trading companies; this impedes online banking, results in blocked accounts, and expands the length and costs of transactions to cover banking and entrepreneurial risks because of the threat of secondary sanctions. Consequently, not only directly listed entities but also people of the targeted countries, their businesses and other partners, humanitarian NGOs and their beneficiaries in targeted and other countries are affected. The easy access to cyber means to distribute negative information makes the reputation risk and the amount of over-compliance even greater.

The existence of a single or a few providers of online banking services (SWIFT), technology and software makes other countries and their national and legal entities more vulnerable. It appears that countries have started to develop alternative processes that, in the long term, undermine cooperation and integration schemes. Impediments to online bank transfers and e-commerce have very strong extraterritorial effects that go counter to the traditional standards of states' jurisdiction. They also undermine the economies of targeted states, impede the ability of these states to develop their economies further and guarantee the well-being of their populations, and violate the expanding number of human rights that appear to be especially clear in the course of the COVID-19 pandemic.

In accordance with the general rules of international trade, the right of final consumers to have access to publicly offered paid or non-paid cyber software or services shall not be limited. Preventing access to specific Internet resources goes counter to the whole scope of so-called 'human rights in the Internet': access to information, freedom of expression, the right to privacy, the right to education and the right to reputation, and also 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 the right to life in emergency situations; it constitutes *de facto* discrimination against targeted societies constituting around 20 per cent of the world population. It also goes counter to repeated calls of the United Nations and other organizations for solidarity, cooperation and multilateralism.

The development of digital technologies affects today all aspects of the introduction and implementation of sanctions, which mostly take the form of unilateral ones, the legality of which is rather dubious from the perspective of international law. Any measures shall be taken by states in the first place within generally recognized standards of international law with due account for their possible humanitarian impact and for the human rights of every individual concerned.