Article

A Critical Analysis of the Need for a Stronger International Legal Framework for Cyber Ethics in Times of Pandemic[1]

Nataliya MAROZ[1]*

[1] Belarusian State University, nataliya.maroz@gmail.com
* Correspondence: nataliya.maroz@gmail.com

Abstract: *Cyber technologies have changed both social and international relations dramatically. The influence of information and telecommunication technologies (hereafter – ICTs) extends from daily life to fundamental freedoms, economies, public administration and political relations. Recent changes brought by coronavirus has emphasized the world's heavy dependence on ICTs. The technologies provide a virtual environment for normal working processes, ensure e-procurement for medical equipment and supplies, raise awareness of coronavirus prevention, maintain people's life at hospitals etc. However, ICTs not only provide considerable benefits to society as a whole, but also can be used for criminal purposes as well as in manner inconsistent with the Charter of the United Nations to inflict substantial damage to critical infrastructure of a state, interfere in elections, block e-government and bank services etc. The pandemic has led to the introduction of new cyber challenges and risks. At the same time, there is no international treaty on cybersecurity as well as on combating cybercrime concluded under the auspices of the United Nations that could be applicable to cope with these newly emerged threats. In this situation, cybersecurity challenges might be addressed through ethical norms, which are more flexible than international legal norms. Thus, in the absence of comprehensive legal response to cyber risks cyber ethics is particularly important.*

Therefore, the article analyzes international legal basis for international cyber ethics. It distinguishes the types of international relations that are regulated by ethical norms. The research defines new risks to cyber security that have emerged during the pandemic and discusses possible ways to respond them through cyber ethics. The paper expresses a view that ethical rules concerning friendly and responsible state behaviour in the context of combating cybercrime should be reflected in an international convention on countering the use of information and communications technologies for criminal purposes, which is going to be developed under the auspices of the United Nations.

Keywords: *cyber ethics, international morality, international law, cybersecurity, human rights*

Citation: Maroz, N. (2021). A Critical Analysis of the Need for a Stronger International Legal Framework for Cyber Ethics in Times of Pandemic. *Revista Etică şi Deontologie*, (*1)*1, 60-73
https://doi.org/10.52744/RED.2021.01.08

Publisher's Note: RED stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

[1] Articol prezentat în cadrul Conferinței Internaționale Valorile Etice în Societatea Actuală – VESA 2021 (3-5 iunie).

1. Introduction

Cyber technologies are widely used almost in all areas of social activities. Their influence extends from daily life to fundamental freedoms, economies, public administration and political relations. The pandemic restrictions have only increased the world's heavy dependence on information and telecommunication technologies. This trend not only brings new challenges and risks to international and national security of states, but also has a considerable influence on international relations. For instance, due to the COVID-19 pandemic meetings at the UN (The Week Ahead at the United Nations, 2021; Wang Yi Chairs UN Security Council High-Level Meeting, 2021; Associated Press, 2020) and other international organizations (the World Health Organization (Seventy-Fourth World Health Assembly, 2021), the Organization for Security and Co-operation in Europe (hereafter – OSCE) (Parry, 2021), the European Union (Video Conference of the Members of the European Council, 25 March 2021, 2021), the Eurasian Economic Union (Заседание Высшего Евразийского экономического совета 21 мая 2021 года, 2021) often take place remotely.

Unfortunately, such extensive use of technologies has provided more opportunities to misuse them for unlawful purposes. The pandemic has witnessed the growth in number of cyber attacks conducted by states (Konrad-Adenauer-Stiftung e.V. & Wiggen, 2020) and non-state actors (Konrad-Adenauer-Stiftung e.V. & Wiggen, 2020); an extending practice of the application of cyber sanctions (Pomaroli & Hammerschmid, 2020); new human rights challenges (OHCHR | Web Summit - Human Rights in the Digital Era, 2021); misinformation campaigns conducted via Internet (Research Paper et al., 2021), the growing digital divide (Coronavirus reveals need to bridge the digital divide | CNUCED, 2020) etc.

International legal framework for state behaviour in cyber space is based on conventions of general character (the Unites Nations (hereafter – UN) Charter, human rights treaties, international humanitarian law treaties etc.), that don't specifically address cyber issues. International treaties on cybersecurity as well as conventions against cybercrime concluded at regional level contain different rules for international cooperation in the area discussed (Maroz, 2019). The UN has just only started the process of the development of a convention on countering the use of information and communications technologies for criminal purposes (Cybercrime Ad Hoc Committee, 2021). However, that is an important step in establishing international legal framework for combating cybercrime.

Unfortunately, there is no effective global consensus concerning the rules governing state behaviour in cyber space even from soft law perspective (UN GGE and OEWG | GIP Digital Watch Observatory for Internet Governance and Digital Policy, n.d.). Therefore, cyber ethics for interstate relations might be an instrument that could respond flexibly to many of newly emerged threats.

International ethics looks at moral values as an essential element of international relations (Shapcott, 2013). However, cyber issues are rarely viewed in the context of international ethics (Dudley et al., 2011). At the same time, cyber technologies are more frequently used to conduct global policy as well as are subject to political decisions within the framework of international relations.

Therefore, the present paper discloses the sources of morality for cyber activities in international relations; defines their applicability to the changing international relations in times of pandemic; reveals those areas in respect to which unwritten ethical norms are not effective enough and should be embodied in international treaty.

The research mainly addresses legal and ethical norms that are adopted at universal level and, thus, doesn't deal with regional approaches to cybersecurity. The article doesn't analyze professional behaviour of international public servants from ethical perspective and considers only international relations between states and international intergovernmental organizations.

2. Sources of international morality for international relations in the area of cyber security

Despite the fact international community consists of different states that have their own moral values and standards of socially accepted behaviour, there are some common moral principles that all states share (truth and justice as well as agreement about such fundamental norms as the dignity of human persons, freedom from torture, impartial application of the law, and freedom of conscience) (Amstutz, 2013). In accordance with a theory of international ethics, these rules refer to as „minimal" morality (Amstutz, 2013).

Regardless a philosophical theory that a certain researcher belongs to, the principles of international law set forth in the UN Charter as well as jus cogens norms are in fact agreed to be not only legal, but also moral standards for international relations. They include such principles as sovereign equality; the settlement of international disputes by peaceful means; refraining in international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the UN; respect for human rights and fundamental freedoms; non-intervention in the internal affairs of other States; the duty of States to co-operate with one another in accordance with the Charter; the principle of equal rights and self-determination of peoples; the principle that States shall fulfil in good faith the obligations assumed by them in accordance with the UN Charter (United Nations Charter, paras 1-2; United Nations General Assembly resolution 2625 (XXV)).

Non-exhaustive list of jus cogens norms summarized by the International Law Commission includes: the prohibition of aggression; the prohibition of genocide; the prohibition of crimes against humanity; the basic rules of international humanitarian law; the prohibition of racial discrimination and apartheid; the prohibition of slavery; the prohibition of torture; the right of self-determination (International Law Commission, 2019).

Nevertheless, international relations are evolving over time and hard law not always can cape pace with these changes. The UN and it specialized agencies as well as regional intergovernmental organizations put their effort in establishing soft law regulation for ethical use of information and telecommunication technologies (hereafter – ICTs) and issues related to them (responsibility of IT business for security by design, ethical aspects of artificial intelligence, automated processing of big data etc.) (UNESCO, 2021; United Nations, 2011; United Nations, 2021; Committee of Ministers of the Council of Europe, 2016). However, new challenges brought by the pandemic require rethinking of some rules in this area. In fact, it's unclear whether new moral principles for international relations have emerged in times of pandemic and whether the content of the existing political values with regard to the use of ICTs are still the same.

Since ethics is „the moral correctness of specified conduct" (Oxford University Press (OUP), n.d.), it defines what conduct should be right (Popa, 2019, p. 428). In other words, it's about what is to be and not about what exists. As Amstutz notes there are three types of actors involved in the development of ethical foreign policy: a) a political leader with strong moral values; b) civil society; c) international organizations (Amstutz, 2013).

From international perspective, states and other subjects of international law are those responsible for the development of international morality. However, as it has been mentioned in the second report by the Group of governmental experts on developments in the field of information and telecommunications in the context of international security „effective cooperation would benefit from the appropriate participation of the private sector and civil society" (Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2013). Thus, private actors such as IT companies, NGOs can influence international ethics.

3. Challenges brought by the pandemic to international relations and international cyber ethics

International relations have witnessed dramatic changes during the pandemic. Among the most important issues of concern are the growing number of state sponsored cyber attacks, unpredictable adverse impact of cyber sanction on the enjoyment of human rights, the lack of legal regulation for international cooperation in combating cybercrime and human rights implications of the COVID-19 cyber-related restrictive measures taken by states.

The number of state sponsored cyber attacks increased during the pandemic (ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected, 2020). At the beginning of the pandemic state-sponsored hackers were allegedly involved in cyber espionage to steal vaccine research in the UK, USA and Canada (Kelion, 2020; Bartlett & Ophel, 2021). Australia became a victim of the attack carried out by „a sophisticated state-based cyber actor" (Jackson, 2020). At the same time, not always any convincing facts of state involvement in cyber attacks were presented (Интерфакс, 2021). Evidentially, unlawful state acts committed with the use of ICTs alongside with the lack of trust and

confidence between states do not assist in enhancing open, secure, peaceful and accessible cyberspace.

International law, and in particular the UN Charter, is applicable and essential to maintaining peace and stability and promoting secure ICT environment (Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 2021). Nevertheless, international law doesn't comprehensively deal with many important issues concerning qualification of cyber attacks, problems of attribution from technical perspective, measures of self-help against state sponsored cyber attacks etc. (Delerue, 2021, p. 4-5, 55). On the other hand, the norms of international morality embodied in the reports of the UN Groups of governmental experts on advancing responsible state behaviour in cyberspace in the context of international security (hereafter – GGE) of 2013, 2015, 2021 address most of these important questions.

In particular, the UNGGE Report of 2013 affirmed the applicability of international law to state conduct within ICT-related activities (art. 19-20), recognized the need for states to „meet their international obligations regarding internationally wrongful acts attributable to them" (art. 23) (Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2013).

UNGGE Report of 2015 significantly expanded the scope of internationally expected measures that state should take in the face of cyber attacks. In particular, the Report of 2015 stipulated that „in case of ICT incidents, states should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences" (art. 13 (b)); „states should be committed to refraining from launching cyberattacks on the critical infrastructures of other states" (art. 13 (b)); „states should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams of another State. A State should not use authorized emergency response teams to engage in malicious international activity" (art. 13 (k)) (Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2015). In more recent reports prepared by the UN Open-ended working group on developments in the field of information and telecommunications in the context of international security (hereafter – OEWG) and the UNGGE these rules have been reiterated and complemented (Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 2021; Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security, 2021).

Unfortunately, states don't consider a possibility of establishing legally binding framework for the standards of responsible state behaviour in cyberspace (Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security, 2021, para. 4). Therefore, for the present time it would be premature to expect treaty-making efforts in the area discussed. Thus, existing international law alongside with norms of international morality continue to be a regulative framework for state behaviour in cyber context.

States are reshaping their possible political responses to malicious cyber activities, what is quite predictable in the light of growing risks of state-sponsored cyber attacks. In 2020 the European Union imposed the first ever sanctions against cyber-attacks (EU Imposes the First Ever Sanctions against Cyber-Attacks, 2020). The USA has been imposing cyber sanctions since 2012 (Bartlett & Ophel, 2021). However, the highest number of sanctions impositions was reached in 2020 (90 designations) (Bartlett & Ophel, 2021).

Sanctions themselves are subjected to an extensive academic debate (Douhan, 2013; Douhan, 2017; Ruys, 2016; Hofer, 2017; Vazquez, 2003; Macfarlane, 2021). Cyber sanctions usually refer to restrictive measures adopted against individuals and entities determined to be responsible for or complicit in malicious cyber-enabled activities (Cyber Sanctions, 2021).

However, cyber sanctions, in fact, can be used to react to any other activities, not connected to cyber-attacks. As Special Rapporteur on the negative impact of unilateral coercive measures on the enjoyment of human rights (hereafter – Special Rapporteur on unilateral coercive measures) stresses „cybertechnologies are also influencing the scope of private entities involved in the implementation of sanctions regimes" (Special Rapporteur on the negative impact of unilateral coercive measures on the enjoyment of human rights, 2020). She indicates, that private entities can be banned from providing certain services or supplying certain software to certain states in accordance with domestic legislation on restrictive measures. For instance, „United States-registered companies block social media accounts as a part of the Magnitsky sanctions regime" (Special Rapporteur on the negative impact of unilateral coercive measures on the enjoyment of human rights, 2020).

As Special Rapporteur on unilateral coercive measures stresses, cyber sanctions had an adverse impact on the enjoyment of basic human rights during the pandemic in Syria. Restrictive measures imposed on Syria in the first pandemic year led to a situation when Syrian government was unable to buy software for CT scanners (Maté, 2021). Syrian population, including medical doctors, was banned from using Zoom, Netflix (France 24, 2021). Moreover, Syrian doctors didn't have a possibility to use other open-access software for distant diagnosis, distant treatment or consultations (for example, PubMed service), what was critical since there were not sufficient doctors in the country (Maté, 2021).

Therefore, unpredictable extraterritorial effect of such sanctions in times of pandemic has adverse influence on the enjoyment of human rights (right to life, right to health, right to work, right to education, right to development and others). Moreover, such measures taking during the pandemic don't contribute to bridging digital divide which is also a special issue of international concern (United Nations, 2021).

Taking into account legal and ethical considerations presented by the Special Rapporteur on unilateral coercive measures in her publications and report it's possible to assume that cyber sanctions having serious adverse humanitarian consequences in times of pandemic can't be considered as morally justified measure regardless the purpose for which they are imposed.

Notably, nowadays not only state-sponsored attacks are challenging national cybersecurity. Hackers attacks became more sophisticates and destructive during the pandemic (Pranggono & Arabo, 2020). They attacked critical infrastructure of states (Burgess, 2020), as well as national and international organizations operating in the fields of healthcare, pharmaceuticals, medical research for different purposes ranging from fraud to espionage (Fighting a War on Two Fronts: COVID-19 Responders and the Threat from Cyberattacks, 2021), committed supply chain attacks (Leyden, 2021).

However, in the lack of applicable international treaties states might not react on transnational cybercrime (Schjølberg & Hubbard, 2005). One of the cases, which demonstrates the need for international cooperation on the matter, is a cyber attack against Colonial Pipeline. Colonial Pipeline was forced to pay $4.4m ransom in cryptocurrency to hackers after cyber attack in May 2021 (Reporter, 2021). The US Intelligence service detected the attack was conducted by hackers from Russia's territory (Mary-Ann Russon, 2021). The US President J.Biden declared that Russia „have some responsibility to deal with this", since the attack had been launched from the territory of Russia (Mary-Ann Russon, 2021).

In fact, the US and Russia don't have an applicable treaty against cybercrime to which both states are parties. At the same time, they are state parties to the UN Convention on transnational organized crime of 2000 (United Nations Convention against Transnational Organized Crime and the protocols thereto, 2004), the Treaty on mutual legal assistance on criminal matters of 1999 (Договор между Российской Федерацией и Соединенными Штатами Америки о взаимной правовой помощи по уголовным делам, 1999) that could be applicable to the issue. Moreover, the dialogue between the two states was established to cooperate on ransomware attackers also owing to political effort (Wilkinson, 2021).

The case of Colonial Pipeline could have been also addressed in the light of due diligence principle, which is well-established in international law. Its applicability to cyber relations was stressed by the UNGGE GGE (Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2015) and substantiated in the Tallinn Manual 2.0 on the international law applicable to cyber operations (Schmitt, 2017, p. 30-50).

Thus, the rule that „states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs" (Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security, 2021) can be viewed both as a legal principle and as a moral obligation of states.

As far as cybercrime is concerned, purely ethical rules (those not enshrined in treaties and binding resolutions of the UN Security Council) are not enough to establish a robust mechanism of international cooperation in the area.

First of all, the collaboration of law-enforcement agencies includes certain procedures that require strict adherence to human rights (right to liberty, right to private life, freedom of movement etc.) and principles of criminal law pursuant to them, such as principle of legality, equality before the law, humanity, fairness, presumption of innocence and others. They are chiefly regulated by law.

Secondly, a power to exercise criminal jurisdiction traditionally belongs to any state. In other words, it emanates from state sovereignty (Beale, 1923, p. 241-262).

Therefore, lacking harmonized criminal law and some important treaty rules (principle aut dedere aut judicare, provisions concerning jurisdiction and mutual legal cooperation, extradition etc.) it's impossible for law-enforcement agencies to cooperate promptly and to the widest extent possible for the purposes of combating cybercrime. The only way to collaborate in such a situation might be to invoke informal procedures of cooperation (Boister, 2012, p. 23; Управление ООН по наркотикам и преступности, 2013, p. XII), which are not effective enough to deal with transnational cybercrime in the absence of applicable international instrument (Cerezo et al., 2007).

Therefore, international ethics is unlikely to be a workable solution to a problem of cybercrime. The International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, which is going to be developed under the aegis of the UN (Mesquita et al., 2020), can be seen as a significant step in strengthening international cooperation in the fight against cybercrime.

Another issue of international concern is human rights impacts of COVID-19 (Wong, 2020). As UN Secretary-General António Guterres put it, „the world faces a pandemic of human rights abuses in the wake of Covid-19" (Guterres, 2021). The most affected human rights include right to life, to health, to education; an adequate standard of living including food, housing, water and sanitation; right to social security; right to work (and protections at work); freedoms of movement, right to private life and freedoms of peaceful assembly and association; freedom of speech.

The use of ICTs in the course of pandemic restrictions resulted in the limitations of human rights (Guterres, 2021). States have been applying different technologies (special software, drones, cameras at public places etc.) for the detection of individuals under quarantine obligations or for observance of social distancing at public places (Sekalala et al., 2020). The extensive use of such technologies have raised many concerns concerning their compatibility with human rights (Sekalala et al., 2020; Brown & Toh, 2021.

Human rights in digital era has been a special issue for consideration by the UN General Assembly (United Nations, 2018; United Nations, 2017; United Nations, 2015), the UN Council on Human Rights (Human Rights Council, 2016; Human Rights Council, 2019), the OSCE (Akdeniz, 2016; OSCE, 2018), Council of Europe (Committee of Ministers, 2019; Committee of Ministers, 2020; Committee of Ministers, 2021; Committee of Ministers, 2018) etc. The legal framework for these rights includes a substantive number of treaties (The Convention on the Prevention and Punishment of the Crime of Genocide 1948, International Covenant on Civil and Political Rights 1966, International Covenant on Economic, Social and Cultural Rights 1966, Convention on the Elimination of All Forms of Discrimination against Women 1979 etc.). Legal obligations emanating from such conventions have a very strong moral basis.

Taking into account the scope and the scale of application of ICTs during the pandemic the following questions have drawn special attention of the UN Human Rights Council special procedures: disinformation and misinformation concerning the pandemic on the Internet (Special Rapporteur on the promotion and protection of the

right to freedom of opinion and expression, 2021); pandemic and freedom of expression (Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 2020), data protection and surveillance in the context of anti-COVID-19 measures (Special Rapporteur on the right to privacy, 2020), artificial intelligence and privacy, and children's privacy (Special Rapporteur on the right to privacy, 2021), digital barriers faced by older persons to community engagement in times of pandemic (Human Rights Council, 2020) and others. The recommendations made by the Special Rapporteurs on human rights alongside with extensive soft law regulation developed by the UN bodies constitute a necessary regulative basis for ethical behaviour of state in the context of newly emerged challenges to human rights.

4. Conclusions

All the aforementioned makes it possible to come to the following conclusions:

1. International ethics is an important part of international normative framework for international relations. Despite the fact international moral norms are not binding for states they're establishing an internationally accepted standards of behaviour for international actors. Therefore, this kind of norms play a significant role for regulating new areas of international relations, such as those concerning the use of ICTs.

2. Unpredictable extraterritorial effect of cyber sanctions in times of pandemic has adverse influence on the enjoyment of basic human rights. Thus, cyber sanctions leading to serious negative humanitarian consequences can't be considered as morally justified measure regardless the purpose for which they are imposed.

3. International cooperation in the fight against transnational cybercrime can not be regulated exclusively by international norms of morality. Clear obligations concerning jurisdiction, mutual legal cooperation and extradition should emanate from legally binding treaty. Moreover, any request for mutual legal assistance or extradition requires compliance with human rights guarantees. Therefore, the widest cooperation in combating cybercrime is possible only within the framework of international treaty. Thus, any informal cooperation in the area discussed can only positively complement international collaboration based on international conventions. Taking into consideration the fact there is no international treaty against cybercrime concluded at universal level, the International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, which is going to be developed under the aegis of the UN, can be seen as a significant step in strengthening international cooperation in the fight against cybercrime.

References

The Week Ahead at the United Nations, (2021), United Nations. https://www.un.org/sg/en/content/the-week-ahead-the-united-nations

Wang Yi Chairs UN Security Council High-level Meeting, (2021), United Nations. https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1874352.shtm

Associated Press, (2020, September 2), *UNSC to meet online to discuss post-COVID global security threats on Sept 24*. Business Today. https://www.businesstoday.in/latest/world/story/unsc-to-meet-online-to-discuss-post-covid-global-security-threats-on-sept-24-271947-2020-09-02

UN General Assembly to be held online, (2021), Global Times. https://www.globaltimes.cn/content/1191309.shtml

Seventy-fourth World Health Assembly, (2021), World Health Organization. https://www.who.int/about/governance/world-health-assembly/seventy-fourth-world-health-assembly

Parry, N., (2021), *Swedish parliamentarian Margareta Cederfelt elected Assembly President at OSCE PA Remote Session*. OSCE PA. https://www.oscepa.org/en/news-a-media/press-releases/press-2021/swedish-parliamentarian-margareta-cederfelt-elected-assembly-president-at-osce-pa-remote-session

Video conference of the members of the European Council, 25 March 2021, (2021, March 25), European Council. https://www.consilium.europa.eu/en/meetings/european-council/2021/03/25/

Заседание Высшего Евразийского экономического совета 21 мая 2021 года, (2021), ЕЭК. https://eec.eaeunion.org/news/zasedanie-vysshego-evrazijskogo-ekonomicheskogo-soveta-ot-21-maya-2021/

Konrad-Adenauer-Stiftung e. V., & Wiggen, J., (2020, June), *The impact of COVID-19 on cyber crime and state-sponsored cyber activities* (No. 391). https://www.kas.de/documents/252038/7995358/The+impact+of+COVID-19+on+cyber+crime+and+state-sponsored+cyber+activities.pdf/b4354456-994b-5a39-4846-af6a0bb3c378?version=1.0&t=1591354291674

Pomaroli, L., & Hammerschmid, I., (2020, May 22), *EU extends cyber sanctions regime in response to increased COVID-19-related cyber threats*. Passle. https://riskandcompliance.freshfields.com/post/102g7x4/eu-extends-cyber-sanctions-regime-in-response-to-increased-covid-19-related-cyber

OHCHR | Web Summit - Human Rights in the Digital Era, (2021), The Office of the High Commissioner for Human Rights. https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=26576&LangID=E

Wong, W.H., (2020, May 7), *Technology threatens human rights in the coronavirus fight*. The Conversation. https://theconversation.com/technology-threatens-human-rights-in-the-coronavirus-fight-136159

Hakmeh, J., Taylor, E., Peters, A., & Ignatidou, S., (2021, February), Research Paper, *The COVID-19 pandemic and trends in technology. Transformations in governance and society*. Chatham House. https://www.chathamhouse.org/sites/default/files/2021-02/2021-02-16-covid-19-trends-technology-hakmeh-et-al.pdf

Coronavirus reveals need to bridge the digital divide | CNUCED, (2020), CNUCED. https://unctad.org/fr/node/2368

Maroz, N., (2019), Regionalization of international cooperation in the fight against cybercrime. *Law Review*, *X*(2), 218–229. http://www.internationallawreview.eu/fisiere/pdf/Nataliya-Maroz-Law_Review_2_2019-19.pdf

Cybercrime Ad Hoc Committee, (2021), United Nations : Office on Drugs and Crime. https://www.unodc.org/unodc/en/cybercrime/cybercrime-adhoc-committee.html

UN GGE and OEWG | GIP Digital Watch observatory for Internet governance and digital policy, (n.d.), DigWatch. Retrieved July 13, 2021, from https://dig.watch/processes/un-gge#view-7541-3

Shapcott, R., (2013), *International ethics* (1st ed.), Wiley. https://www.perlego.com/book/1535226/international-ethics-pdf

Dudley, A., Braman, J., & Vincenti, G., (2011), *Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices,* (1st ed.), IGI Global.

Amstutz, M.R., (2013), *International Ethics: Concepts, Theories, and Cases in Global Politics* (Fourth ed.), Rowman & Littlefield Publishers.

Charter of the United Nations, 1945, 1 UNTS XVI.

United Nations General Assembly resolution 2625 (XXV), Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, A/RES/2625 (XXV) (24 October 1970), available from https://unispal.un.org/DPA/DPR/unispal.nsf/0/25A1C8E35B23161C852570C4006E50AB

International Law Commission, (2019), *Peremptory norms of general international law (jus cogens)* (text of the draft conclusions and draft annex provisionally adopted by the Drafting Committee on first reading). https://documents-dds-ny.un.org/doc/UNDOC/LTD/G19/147/22/PDF/G1914722.pdf?OpenElement

UNESCO, (2021, March), *Final report on the draft text of the recommendation on the ethics of artificial intelligence*. https://unesdoc.unesco.org/ark:/48223/pf0000376712

Unites Nations, (2011), *Guiding Principles on Business and Human Rights*. United Nations Human Rights Office of the High Comissioner. https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

Unites Nations, (2021, January), *Access to remedy and the technology sector: basic concepts and principles. A B-Tech Foundational Paper*. United Nations Human Rights Office of the High Commissioner. https://www.ohchr.org/Documents/Issues/Business/B-Tech/access-to-remedy-concepts-and-principles.pdf

Committee of Ministers of the Council of Europe recommendation, Human rights and business, (CM), Rec. CM/Rec(2016)3 (2 March 2016), available from https://rm.coe.int/human-rights-and-business-recommendation-cm-rec-2016-3-of-the-committe/16806f2032

Oxford University Press (OUP), (n.d.), *Ethics*. Lexico.Com. Retrieved July 13, 2021, from https://www.lexico.com/definition/ethics

Popa, P., (2019), *Elements that impose limits on international ethics*, CES Working Papers, ISSN 2067-7693, Alexandru Ioan Cuza University of Iasi, Centre for European Studies, Iasi, 10 (4), 423–437

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, (2013, June), *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/68/98), UN General Assembly. https://undocs.org/A/68/98

ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected, (2020, October), EU Agency for Cybersecurity. https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

Kelion, L.F.C.B., (2020, July 16), *Coronavirus: Russian spies target Covid-19 vaccine research*. BBC News. https://www.bbc.com/news/technology-53429506; *Sanctions by the Numbers: Spotlight on Cyber Sanctions*. (2021, May 4). Center for a New American Security (En-US). https://www.cnas.org/publications/reports/sanctions-by-the-numbers-cyber

Jackson, J., (2020, June 19), *Australia under cyberattack: is the world facing a cyber pandemic?,* Finfeed. https://finfeed.com/features/australia-under-cyberattack-world-facing-cyber-pandemic/

Интерфакс, (2021, April 7), *В Совбезе посетовали, что США выставили РФ кибер-агрессором без доказательств*. Интерфакст. https://www.interfax.ru/world/760028

Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, (2021, March), *Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/75/816). United Nations General Assembly. https://undocs.org/en/A/75/816

Delerue, F., (2021), *Cyber Operations and International Law (Cambridge Studies in International and Comparative Law, Series Number 146)*, Cambridge University Press.

Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security, (2021, May), *Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security* (Advance copy). https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, (2015, July), *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/70/174). United Nations General Assembly. https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

EU imposes the first ever sanctions against cyber-attacks, (2020, July 30), European Council. https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/

Bartlett, J., & Ophel, M., (2021, May 4), *Sanctions by the Numbers: Spotlight on Cyber Sanctions*. Center for a New American Security (En-US). https://www.cnas.org/publications/reports/sanctions-by-the-numbers-cyber

Douhan, A., (2013), *Unilateral Coercive Measures: Criteria and Characteristics*. http://www.ohchr.org/Documents/Events/WCM/AlenaDouhan.doc

Douhan, A., (2017), Fundamental human rights and coercive measures: impact and interdependence, *J. Belarus. State Univ. Int. Relat*, *1*, 67–77

Ruys, T., (2016), Sanctions, Retorsions and Countermeasures: Concepts and International Legal Framework. *SSRN Electronic Journal*. Published. https://doi.org/10.2139/ssrn.2760853

Hofer, A., (2017), The Developed/Developing Divide on Unilateral Coercive Measures: Legitimate Enforcement or Illegitimate Intervention?, *Chinese Journal of International Law*, *16*(2), 175–214. https://doi.org/10.1093/chinesejil/jmx018

Vazquez, C.M., (2003), TRADE SANCTIONS AND HUMAN RIGHTS - PAST, PRESENT, AND FUTURE. *Journal of International Economic Law*, *6*(4), 797–839. https://doi.org/10.1093/jiel/6.4.797

Macfarlane, E., (2021), Strengthening Sanctions: Solutions to Curtail the Evasion of International Economic Sanctions Through the Use of Cryptocurrency. *Michigan Journal of International Law*, *42.1*, 199. https://doi.org/10.36642/mjil.42.1.strengthening

Cyber Sanctions, (2021, January 11), United States Department of State. https://www.state.gov/cyber-sanctions/

Special Rapporteur on the negative impact of unilateral coercive measures on the enjoyment of human rights, (2020, July), *Negative impact of unilateral coercive measures: priorities and road map*, Human Rights Council. https://undocs.org/en/A/HRC/45/7

Maté, A., (2021, January 14), *UN expert: crippling US sanctions on Syria are illegal and hurting civilians*. The Grayzone. https://thegrayzone.com/2021/01/14/un-expert-crippling-us-sanctions-on-syria-are-illegal-and-hurting-civilians/

France 24, (2021, March 19), *In pandemic year, Syrians blocked from Zoom, Netflix*. France 24. https://www.france24.com/en/live-news/20210319-in-pandemic-year-syrians-blocked-from-zoom-netflix

Don't let the digital divide become 'the new face of inequality': UN, (2021, April 29), UN News. https://news.un.org/en/story/2021/04/1090712; *Coronavirus reveals need to bridge the digital divide | CNUCED*. (2020b, April 6). CNUCED. https://unctad.org/fr/node/2368

Pranggono, B., & Arabo, A., (2020), COVID -19 pandemic cybersecurity issues. *Internet Technology Letters*, *4*(2). https://doi.org/10.1002/itl2.247

Burgess, M., (2020, March 22), *Hackers are targeting hospitals crippled by coronavirus*. WIRED UK. https://www.wired.co.uk/article/coronavirus-hackers-cybercrime-phishing

Fighting a war on two fronts: COVID-19 responders and the threat from cyberattacks, (2021, June 23), Aon. https://www.aon.com/cyber-solutions/thinking/fighting-a-war-on-two-fronts-covid-19-responders-and-the-threat-from-cyberattacks/

Leyden, J., (2021, April 16), *Behind the Great Firewall: Chinese cyber-espionage adapts to post-Covid world with stealthier attacks*. The Daily Swig | Cybersecurity News and Views.

https://portswigger.net/daily-swig/behind-the-great-firewall-chinese-cyber-espionage-adapts-to-post-covid-world-with-stealthier-attacks

Schjølberg, S., & Hubbard, A.M., (2005, June 28–July 1), *Harmonizing national legal approaches on cybercrime* [Paper presentation]. WSIS Thematic Meeting on Cybersecurity, Geneva, Switzerland. https://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf

Reporter, G.S., (2021, May 20), *Colonial Pipeline confirms it paid $4.4m ransom to hacker gang after attack*. The Guardian. https://www.theguardian.com/technology/2021/may/19/colonial-pipeline-cyber-attack-ransom

Uberti, D., (2021, June 11), *How the FBI Got Colonial Pipeline's Ransom Money Back*. WSJ. https://www.wsj.com/articles/how-the-fbi-got-colonial-pipelines-ransom-money-back-11623403981

Mary-Ann Russon, B., (2021, May 10), *US fuel pipeline hackers „didn't mean to create problems."* BBC News. https://www.bbc.com/news/business-57050690

(2004), United Nations Convention against Transnational Organized Crime and the protocols thereto, New York: United Nations.

(1999), Договор между Российской Федерацией и Соединенными Штатами Америки о взаимной правовой помощи по уголовным делам, Москва: Министерство иностранных дел Российской Федерации.

Wilkinson, B.H., (2021, June 17), *Here's what happened at the Biden-Putin Geneva summit*, CNN. https://edition.cnn.com/world/live-news/biden-putin-meeting-geneva-updates-intl/index.html

Коммерсантъ, (2021, May 13). *Байден рассказал о контакте с Россией после атаки на Colonial Pipeline*. Коммерсантъ. https://www.kommersant.ru/doc/4804784

Schmitt, M. (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (pp. 30-50). (2nd ed). Cambridge: Cambridge University Press.

Beale, J.H., (1923), The Jurisdiction of a Sovereign State, *Harvard Law Review*, 36(3), 241. https://doi.org/10.2307/1329779

Boister, N., (2012), *An Introduction to Transnational Criminal Law* (1st ed.). Oxford University Press.

Управление ООН по наркотикам и преступности, (2013, February), *Всестороннее исследование проблемы киберпреступности*. Организация Объединенных Наций. https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Russian.pdf

Cerezo, A.I., Lopez, J., & Patel, A., (2007), International Cooperation to Fight Transnational Cybercrime, *Second International Workshop on Digital Forensics and Incident Analysis (WDFIA 2007)*, Published. https://doi.org/10.1109/wdfia.2007.4299369

Mesquita, J.B., Kapilashrami, A., & Meier, B.M., (2020, October), *Human rights dimensions of the COVID-19 Pandemic* (Background paper 11), The University of North Carolina at Chapel Hill. https://theindependentpanel.org/wp-content/uploads/2021/05/Background-paper -11-Human-rights.pdf

Guterres, A., (2021, February 25), *The world faces a pandemic of human rights abuses in the wake of Covid-19*, The Guardian, https://www.theguardian.com/global-development/2021/feb/22/world-faces-pandemic-human-rights-abuses-covid-19-antonio-guterres

Sekalala, S., Dagron, S., Forman, L., & Meier, B.M., (2020), Analyzing the human rights impact of increased digital public health surveillance during the COVID-19 crisis, *Health and Human Rights Journal*, *22*(2), 7–20.

Brown, D., & Toh, A., (2021, March 4), *Technology is Enabling Surveillance, Inequality During the Pandemic*, Human Rights Watch, https://www.hrw.org/news/2021/03/04/technology-enabling-surveillance-inequality-during-pandemic

Mobile Location Data and Covid-19: Q&A, (2020, October 28), Human Rights Watch. https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa

General Assembly resolution 73/179, *The right to privacy in the digital age*, A/RES/73/179 (17 December 2018), available from https://undocs.org/en/A/RES/73/179

General Assembly resolution 71/199, *The right to privacy in the digital age*, A/RES/71/199 (25 January 2017), available from https://undocs.org/en/A/RES/71/199

General Assembly resolution 69/204, *Information and communications technologies for development*, A/RES/69/204 (21 January 2015), available from https://undocs.org/en/A/RES/69/204

Human Rights Council resolution 32/13, *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/32/L.20 (1 July 2016), available from https://digitallibrary.un.org/record/845728/files/A_HRC_32_L-20-EN.pdf

Human Rights Council resolution 42/15, *The right to privacy in the digital age*, A/HRC/RES/42/15 (26 September 2019), available from https://digitallibrary.un.org/record/3837297/files/A_HRC_RES_42_15-EN.pdf

Akdeniz, Y., (2016, March), *Media freedom on the Internet* (An OSCE Guidebook). OSCE Representative on Freedom of the Media. https://www.osce.org/files/f/documents/3/c/226526.pdf

OSCE, (2018, January), *International standards and comparative approaches on freedom of expression and blocking of terrorist or extremist content online* (the OSCE Representative on Freedom of the Media on the request of the Russian Federation). https://www.osce.org/files/f/documents/9/5/384564.pdf

Committee of Ministers of the Council of Europe, *Declaration On the manipulative capabilities of algorithmic processes,* Decl(13/02/2019)1 (13 February 2019), available from https://search.coe.int/cm/pages/result_details.aspx?objectid=090000168092dd4b

Committee of Ministers of the Council of Europe, *Recommendation on the human rights impacts of algorithmic systems*, CM/Rec(2020)1 (8 April 2020), available from https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154

Committee of Ministers of the Council of Europe, *Guidelines on upholding equality and protecting against discrimination and hate during the Covid-19 pandemic and similar crises in the future*, CM(2021)37-add1final (5 May 2021), available from https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680a25afc

Committee of Ministers of the Council of Europe recommendation, *Guidelines to respect, protect and fulfil the rights of the child in the digital environment*, CM/Rec(2018)7 (4 July 2018), available from https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016808b79f7

Committee of Ministers of the Council of Europe, *Recommendation on the roles and responsibilities of internet intermediaries*, CM/Rec(2018)2 (7 March 2018), available from https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680790e14

Disinformation and freedom of opinion and expression, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, (2021, April), Human Rights Council. https://undocs.org/A/HRC/47/25

Disease pandemics and the freedom of opinion and expression, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. (2020, April). Human Rights Council. https://www.undocs.org/A/HRC/44/49

Preliminary evaluation of the privacy dimensions of the coronavirus disease (COVID-19) pandemic, Report of the Special Rapporteur on the right to privacy, (2020, July), Human Rights Council. https://undocs.org/A/75/147

Artificial intelligence and privacy, and children's privacy, Report of the Special Rapporteur on the right to privacy, (2021, January), Human Rights Council. https://undocs.org/A/HRC/46/37

Human Rights Council, *Impact of the coronavirus disease (COVID-19) on the enjoyment of all human rights by older persons, Report of the Independent Expert on the enjoyment of all human rights by older persons* (2020, July), available from https://undocs.org/A/75/205