UNIVERSIDAD DE MURCIA

http://revistas.um.es/analesderecho

ANALES de DERECHO

The Various Dimensions of Cyberthreats: (In)consistencies in the Global Regulation of Cybersecurity

TATIANA NASCIMENTO HEIM

PhD Researcher at the University of Twente, The Netherlands

RAMSES A. WESSEL

Professor of European Law, University of Groningen, The Netherlands

Las dimensiones de las ciberamenazas: Inconsistencias de la regulación global

Resumen

La revolución de la información permite un acceso amplio y rápido a los datos, pero también permite o amplía la posibilidad de que terceros traten de dañar los sistemas y causar daños. A pesar de la creciente sofisticación de los ataques, el conocimiento técnico del usuario de hecho está disminuyendo. Eso puede explicarse por el hecho de que los scripts de ataque y los kits de herramientas están disponibles de manera asequible, con efectos devastadores para la sociedad. Cualquier ordenador con acceso a Internet, hoy en día es vulnerable a amenazas como virus, gusanos y otros ataques. Las amenazas a la ciberseguridad son difíciles de clasificar, ya que las diferentes categorías se superponen y las actividades pueden derivarse de un solo sujeto o de actores y grupos complejos y globales. Las amenazas cibernéticas se diferencian de los problemas de seguridad tradicionales, principalmente, en lo que respecta a la atribución de su jurisdicción, ya que un ataque cibernético se puede realizar desde cualquier lugar, sin que el actor tenga que salir de casa. En ese sentido, el enfoque principal del presente documento es revisar las diferentes dimensiones de las ciberamenazas y clasificarlas sobre la base de las definiciones y descripciones utilizadas en los instrumentos internacionales. Todo ello con el fin de establecer (in)coherencias entre las diversas normas. Nuestros hallazgos sugieren que, a pesar de los sistemas regulatorios bastante fragmentados en todo el mundo, existe un acuerdo general sobre las nociones y definiciones básicas. Esto ofrece un buen punto de partida para los debates en curso sobre una mayor armonización de las normas mundiales sobre ciberseguridad y la persecución del ciberdelito.

Palabras clave: *seguridad cibernética; ciberamenazas; regulación mundial; fragmentación; normas internacionales.*

"The Various Dimensions of Cyberthreats: (In)consistencies in the Global Regulation of Cybersecurity"[1]

Abstract

The Information Revolution enables wide and fast access to data but it also creates intruders intending to harm systems and cause damages. Despite the increasing sophistication of the attacks, the technical knowledge of the user is in fact declining. That can be explained by the fact that attack scripts and toolkits are available for beginners with devastating effects for society. Any computer connected to the internet today is vulnerable to threats such as viruses, worms, and other attacks. Cybersecurity threats are difficult to classify as the different categories overlap and the activities can originate from an individual actor or from non-state actors and groups. Cyberthreats differ from traditional security issues mainly with regard to attribution and jurisdiction as a cyberattack can be done from anywhere, without the actor leaving home. In that respect, the main focus of the present paper is to revisit the different dimensions of cyberthreats and to classify them on the basis of definitions and descriptions used in international instruments with a view to establish (in)consistencies between the various norms. Our findings suggest that, despite the quite fragmented regulatory systems around the world, there is to a very large extent agreement on the basic notions and definitions. This offers a good starting point for the ongoing debates on a further harmonisation of the global norms on cybersecurity, such as in the case of cybercrime.

Keywords*: cybersecurity; cyberthreats; global regulation; fragmentation; international norms.*

[1] This article has been produced in the framework of the Jean Monnet Chair on The Transformative Power of European Union Law (TEULP), funded by the European Commission (Project: 101047458 - TEULP - ERASMUS-JMO-2021-HEI-TCH-RSCH) and led by Juan Jorge Piernas López, Professor at the Faculty of Law of the University of Murcia.

SUMARIO: I. INTRODUCTION. II CYBERATTACKS. III. CYBERTERRORISM. IV. CYBERESPIONAGE. V. CYBERWAR. VI. CYBERCRIME. VII. CONCLUSION. VIII. BIBLIOGRAPHY.

I. INTRODUCTION

In a previous research paper, the present authors pointed to the complexities related to the global regulation of cybersecurity.[2] As we argued there, these complexities mainly relate to the fragmentation of actors, definitions and norms. Cybersecurity as a field of public attention has developed rapidly over the past few decades. The piecemeal approach in which separate dimensions of cybersecurity were regulated has led to fragmentation. This fragmentation as such is not a bad thing as it also allows for special rules in special cases and situations. Yet, the further development of the internet and its possibilities have raised calls for a more consolidated approach, which would prevent possible conflicts between norms and would enhance legal certainty. With the many existing (public and private) actors and the many different instruments used, it has become increasingly difficult to understand which norms are applicable in which situation. Moreover, the mentioned fragmentation is believed to have led to diverging rules in different countries and jurisdictions, making it more difficult for states to cooperate in a field that is by its nature 'borderless' and transnational.

While consolidation of the various instruments and norms is indeed difficult, it is not impossible to organise things differently. The European Union has recently done so when it rebranded its Agency for Network and Information Security (ENISA) to the European Union Agency for Cybersecurity, also with the idea to provide it with an overall coordinating role between the EU and its member states.[3] While it is obviously easier to agree on this with 27 states, than with almost 200 globally, the time has come to start thinking about the global regulation of cybersecurity through a combination and perhaps consolidation of the different instruments. Whether a further consolidation is possible depends first of all on the extent to which the mentioned fragmentation is indeed visible in a number of key instruments that currently regulate cybersecurity.

[2] T. NASCIMENTO HEIM AND R.A. WESSEL, 'The Global Regulation of Cybersecurity: A Fragmentation of Actors, Definitions and Norms', in Lucía Millán Moro (dir.) and Gloria Fernández Arribas (ed.), *Ciberataques y Ciberseguridad en la Escena Internacional*, Madrid: Aranzadi Thomas Reuters, 2020, p. 146-173.
[3] https://www.enisa.europa.eu.

In that respect, the main focus of the present paper is to revisit the different dimensions of cyberthreats and to classify them on the basis of definitions and descriptions used in international instruments with a view to establish (in)consistencies between the various norms. In the framework of a larger project on this topic, we have selected a number of key instruments with the aim of comparing the various norm-descriptions and definitions. This selection was based on a thorough analysis of the relevance of the instruments in the regulation of cybersecurity, in which we checked a total of […] instruments.[4] Yet, as we will see, cybersecurity threats are difficult to classify because of the overlapping categories, and the fact that the activities can originate from an individual actor, non-state actors and states. For example, 'hacking' can originate from organised crime, terrorist attacks, or state aggression.[5] Cyberthreats differ from traditional security issues mainly with regard to attribution and jurisdiction as a cyberattack can be performed from anywhere, without the actor leaving home. Therefore, important security and legal notions such as 'self-defence' and 'armed attack' that are based on territorial conceptions are not automatically applicable.[6] Threats to cyberspace can be classified in many ways and are often described differently by authors or organisations.[7]

The following part is divided into five sections, which will used to further analyse the various types of cyberthreats. Section II will first of all aim to shed more light on the notion of cyberattack. Section III will provide an analysis of the instruments that deal with cyberterrorism. This will be followed by Section IV that focusses on cyberespionage. Section V will analyse cyberwar instruments and Section VI will examine cybercrime. We will end by providing a conclusion which aims to provide further insight into the role of these various notions in the global and regional regulation of cybersecurity.

II. CYBERATTACKS

Cyberattacks' may very well be the most well-known dimension of cyber-insecurity. Cyberattacks are often confused with terms like 'cyberwar' and 'cybercrime', but there are many different types of cyberattacks and the concept can be explained from different

[4] A complete overview will be presented in T. NASCIMENTO HEIM, *Global Governance and Regulation of Cybersecurity: Towards Collective Arrangements?*, 2023 (forthcoming)
[5] CORNISH, PAUL, "Cyber security and politically, socially and religiously motivated cyber attacks", *European Parliament*, Brussels, p. 1-32, 2009.
[6] PERNICE, INGOLF, "Cybersecurity governance: Making cyberspace a safer place", *HIIG Discussion Paper Series*, vol. 3, 2017, p. 1-28.
[7] HANSMAN, SIMON, and HUNT, RAY, "A taxonomy of network and computer attacks", *Computers & Security*, 2005, p. 31-43.

perspectives. The term cyberattack encompasses everything from a simple computer attack to full-scale operations with the aim of wreaking physical destruction.[8] The definitions of cybersecurity and cyberattacks are interconnected because the assets that the first one aims to protect, the second has the objective of destroying.[9]

Cyberattacks seem to be proliferating in number, sophistication and severity.[10] Cyberattacks can be defined as: "*deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information resident in or transiting them*".[11] Similarly, Randall argues that cyberattacks are a "*large genus of all kind of attacks on information system. Such attacks include traditional counterespionage and disinformation campaigns, old-fashioned destruction of telephones lines, jamming of radio signals, killing of carrier pigeons*"[12] The targets of a cyberattack can range from a specific system to a national critical infrastructure.[13] For instance, in March 2022, Ukraine was affected by the Russian Federation military invasion. Alongside the armed conflict, there were cyberattacks against Ukraine's digital infrastructure, including the health sector.[14]

In the instruments we selected, the term 'cyberattack' is broadly used as a negative consequence of breaches in the cybersecurity environment. For instance, Resolution 50 of the International Telecommunication Union (ITU) emphasises the need to defend information and telecommunication system against cyberattack.[15] Likewise, the Resolution on the *"Creation of a global culture of cybersecurity and the protection of critical information infrastructures"* explains how critical infrastructure should be defended to recover from cyberattack. [16]

[8] NYE JR, JOSEPH S., *Cyber power*. Harvard Univ Cambridge Ma Belfer Center for Science and International Affairs, 2010.
[9] ARMY TRAINING AND DOCTRINE COMMAND FORTLEAVENWORTH KS DEPUTY CHIEF OF STAFF FOR INTELLIGENCE, *DCSINT Handbook No 1.02*, 2005.
[10]SHACKELFORD, SCOTT J., "Toward cyberpeace: Managing cyberattacks through polycentric governance" *Am. UL Rev.*, vol. 62, 2012, p. 1273.
[11] LIN, HERBERT, "Lifting the veil on cyber offense", *IEEE Security & Privacy*, 2009, p.15-21.
[12] DIPERT, RANDALL R, "The ethics of cyberwarfare", *Journal of Military Ethics*, 2010, p. 384-410.
[13] DE SANTANNA, JOSÉ JAIR CARDOSO, *DDoS-as-a-Service: investigating booter websites*, Enschede, 2017.
[14] SAMARASEKERA, UDANI, *Cyber risks to Ukrainian and other health systems*, 30 March 2022, <https://www.thelancet.com/journals/landig/article/PIIS2589-7500(22)00064-4/fulltext>.
[15] INTERNATIONAL TELECOMMUNICATION UNION, *Resolution 50*, 25 October – 3 November de 2016.
[16] UNITED NATIONS, "Noting Also", *A/RES/58/199*.

Within the selection we made out of a very large set of potentially relevant instruments, Regulation 2019/796, part of the EU's Cyber Diplomacy Toolbox, is the only one that provides a specific provision on cyberattacks. This piece of legislation was promoted by the Netherlands and the United Kingdom after suffering a major cyberattack that was allegedly linked to a Chinese group.[17] One month later, the Council of the European Union adopted legislation that enables sanctions against cyberattacks. The norms allow for sanctions such as the freezing of funds,[18] freezing of economic resources[19] of any natural or legal person, entity, or body responsible for (attempted) cyberattacks with a (potentially) significant effect.[20] The sanctions also establish the principle of due diligence on the basis of which the member states should take the necessary measures to prevent natural persons being affected by cyberattacks through their territories.[21] These sanctions are considered 'smart' because they are directed at individuals and entities instead of broad economic sanctions that affect an entire population of a country.[22]

For that purpose, Annex I contains a list of legal persons, entities, or bodies whose funds shall be frozen and who shall be denied entry into the EU's member states.[23] Furthermore, Regulation 2019/796 defines cyberattacks as actions that involve: *"(a) access to information systems; (b) information system interference; (c) data interference; or (d) data interception"*.[24] Such action should not be authorised by the owner or another holder of the system.[25] The definition of cyberattack of the European Union is thus close to concepts developed in scholarly literature as it concerns the protection of the availability, integrity and confidentiality of the information and the cyber systems. One of the main challenges of the Resolution concerns how to link the person behind the attack and the

[17]BOTEK, ADAM, *European Union establishes a sanction regime for cyber-attack*, https://ccdcoe.org/incyder-articles/european-union-establishes-a-sanction-regime-for-cyber-attacks/
[18] See id. at art. 3(1).
[19] See id. at art. 3(1).
[20] EUROPEN UNION, "Article 4", *Council Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States*, 17 May 2019.
[21] Id. at art. 4.
[22] MIADZVETSKAYA, YULIYA, "Challenges of the Cyber Sanctions Regime Under Common Foreign and Security Policy (CFSP)", *Anton Vedder, Jessica Schroers, Charlotte Ducuing, Peggy Valcke, KU Leuven Centre for IT & IP Law Series*, 2019.
[23] EUROPEN UNION, "Article 3", *Council Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States*, 17 May 2019.
[24] Id. at art. 3.
[25] Id. at art. 3.

geographical area. This is a difficult exercise which has to take into account technical, legal and political areas. [26]

Yet, not only public rules apply; the private sector is also involved in creating norms that regulate cyberattacks. Thus, the so-called Tech Accord uses the same logic as the original Digital Geneva Convention by arguing that private actors have an active role in applying defence measures and will have to abstain from hacking back. One of the principles of the accord is to *"protect all of our users and customers everywhere".*[27] In such a manner, the private sector is both an agent and object of cybersecurity.[28] Unfortunately, the Tech Accord is not clear about what it means to elaborate an active defense and the absence of a definition could encourage aggressive practices. For instance, active defence measures could involve 'honeypots' that are virtual traps that attract attackers. In extreme cases, it could be considered a form of entrapment[29] or even violate privacy laws.

Our first sub-conclusion is that only Regulation 2019/796 and the Tech Accord aim to regulate cyberattacks. We believe that these norms are consistent because both establish responsibilities for the attacker. The EU Regulation establishes restrictive measures against cyberattack when it is threatening the member states, while the Tech Accord focuses on the behaviour of the private sector to combat cyberattacks. The role of the private sector is to prevent/defend the system from cyberattacks where states play a more offensive role by establishing sanctions. However, there are challenges related to the implementation of the norms because of barriers to attributing a cyberattack to an individual or entities, which has to be performed based on technical and intelligence sources. In addition, there is a grey zone between what constitute defence and offence measures and further clarification is needed to define the role of each actor.

III. CYBERTERRORISM

'Cyberterrorism' is also a nebulous concept that is often confused with 'cyberattack', 'cybercrime' and 'cyberwar'. According to the literature, cyberterrorism is a form of

[26] MIADZVETSKAYA, YULIYA, "Challenges of the Cyber Sanctions Regime Under Common Foreign and Security Policy (CFSP)", *S): Anton Vedder, Jessica Schroers, Charlotte Ducuing, Peggy Valcke, KU Leuven Centre for IT & IP Law Series*, 2019.

[27] TECH ACCORD, *Cybersecurity Tech Accord. Protecting Users and Customers Everywhere*, 2018.

[28] PATTISON, JAMES, "From defence to offence: The ethics of private cybersecurity", *European Journal of International Security*, vol. 5, 2020, p. 233-254.

[29] In the American law entrapment is the conception and planning of an offense by an officer and his procurement of its commission by one who would not have perpetrated it except for the trickery, persuasion, or fraud of the officers (this definition was stated by Justica Roberts in 1932 in Sorrells vs. United States.

terrorism using new technologies and networks to conduct operations.[30] Terrorism, in turn, can be defined as "*the unlawful use or threatened use of force or violence by a person or an organized group against people or property with the intention of intimidating or coercing societies or governments often for ideological or political reasons.*"[31] The inclusion of the prefix 'cyber' to the previous concept uses the network as a tool for accomplishing terrorism, and cyberspace as a new place to spread the message. The main goal of cyberterrorism is coercing, intimidating[32] and creating harm,[33] because the main aim of this type of cyberattacks is to create terror.[34]

With a view to the instruments we selected, the European Union in its "EU Cybersecurity Strategy: An open, safe and secure cyberspace" understands cyberterrorism as a type of cybercrime and stresses that socially acceptable crimes such as illegal downloading of movies can help fund terrorism and organised crime.[35] Moreover, the Organization of American States (OAS), in the Declaration Strengthening Cyber-Security in the Americas, condemns terrorism in all forms and manifestations and believes it to be a serious threat for international peace, security, democracy, stability and prosperity.[36]

Meanwhile, Article 15 of the draft Arab Convention on Combating Information Technology Offences provides the following elements:

- dissemination and advocacy of the ideas and principles of terrorist groups;
- financing of and training for terrorist operations and facilitating communication between terrorist organizations;
- dissemination of methods to make explosives, especially for use in terrorist operations; and

[30] ARMY TRAINING AND DOCTRINE COMMAND FORTLEAVENWORTH KS DEPUTY CHIEF OF STAFF FOR INTELLIGENCE, *DCSINT Handbook No 1.02*, 2005.
[31] WARREN, M. J., "Terrorism and the Internet", *Cyber warfare and cyber terrorism*. IGI Global, 2007, p. 42-49.
[32] DENNING, D., "A view of cyberterrorism 5 years later", *Internet security: Hacking, counterhacking, and society*, p. 123, 2007; KENNEY, MICHAEL, "Cyber-terrorism in a post-stuxnet world", *Orbis, vol.* 59, n.1, 2015, p. 111-128.
[33] BRENNER, SUSAN W., "Cybercrime, cyberterrorism and cyberwarfare", *Revue internationale de droit penal*, v.77, n.3, 2006, p. 453-471.
[34] CONWAY, MAURA, "Reality bytes: cyberterrorism and terrorist 'use' of the Internet", *First Monday*, v. 7, n. 11, 2002, p. 1-17.
[35] EUROPEAN UNION, *European Parliament resolution of 12 September 2013 on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013/2606(RSP))*, 12 September 2013.
[36] ORGANIZATION OF AMERICAN STATES, *Declaration strengthening cyber-security in the americas*, 7 de March de 2012.

- spreading religious fanaticism and dissention and attacking religions and beliefs.[37]

It is important to point out that the definition of the Arab Convention not only includes coercing, intimidation and creating harm, but also financing and training for a terrorist purpose. Likewise, the Agreement between the member states of the Shanghai Cooperation Organization has a broader perspective, and information terrorism is described as: *"using information resources in the information space and/or influencing on them for terrorist purposes"*[38] The source of this threat encompasses, inter alia, carrying out terrorist activities, bringing new terrorism supporters, blocking media channels and propaganda and creating an atmosphere of fear. [39] In conclusion, in the various international and regional instruments, there are consistent approaches to situations in which the internet is used to disseminate, finance and spread information for terrorist purposes.

IV. CYBERESPIONAGE

'Cyberespionage' or 'electronic espionage' is the intentional use of information, information processing systems and networks to gain access to sensitive and secret information about an adversary, individuals, groups or governments.[40] The aim of cyberespionage is to obtain[41]/extract[42]/access[43]/get[44]/copy[45] sensitive and protected information. It is important to emphasise that the goal of copying information is fundamental for the act of espionage,[46] and this type of cyberattack is committed

[37] THE LEAGUE OF ARAB STATES, "Article 15", *Arab Convention on Combating Information Technology*, 15 Feb 2012.
[38] SHANGHAI COOPERATION ORGANIZATION, "Information terrorism, List of Basic Terms in the Field of International Information Security", *Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization*, 2009.
[39] Id. at "Information terrorism, List of Basic Terms in the Field of International Information Security", *Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization*, 2009.
[40] UMA, M., AND GANAPATHI PADMAVATHI, "A Survey on Various Cyber Attacks and their Classification", *Int. J. Netw. Secur.*, 2013, p. 390-396.
[41] UMA, M., AND GANAPATHI PADMAVATHI, "A Survey on Various Cyber Attacks and their Classification", *Int. J. Netw. Secur.*, 2013, p. 390-396.
[42] STRUNK, DANIEL, et al., "American Cyber Insecurity: The growing danger of cyber attacks", *Duke University*, Durham, 2014.
[43] BUCHAN, RUSSELL, *Cyber espionage and international law*, Research handbook on international law and cyberspace, Edward Elgar Publishing, 2015.
[44] GREATHOUSE, CRAIG B., "Cyber war and strategic thought: Do the classic theorists still matter?", *Cyberspace and International Relations*, Springer, Berlin, p. 21-40, 2014.
[45] BUCHAN, RUSSELL, *Cyber espionage and international law*, Research handbook on international law and cyberspace, Edward Elgar Publishing, 2015.
[46] Ibid.

regardless of losing or damaging information,[47] or altering the computer.[48] In cyberespionage, the actor observes or copies data and that observation is clandestine, even when the actor does not affect the system or adds false or misleading information.[49]

In the selected instruments, we did not find norms related to cyberespionage, which points to the idea that this type of cyberthreat is largely unregulated. Studies on cyberespionage, however, reveal that the purpose of cyberespionage is to gain political and military[50] or monetary advantage.[51] Thus, Luiijf defines cyberespionage as: "*Cyber or electronic espionage is the intentional use of information processing systems and networks activities in an effort to gain access to sensitive information about an adversary or competitor for the purpose of gaining an advantage or selling the sensitive information for monetary reward."*[52] Likewise, Robinson establishes the purpose of cyberespionage as "*obtaining political or military information covertly"*.[53]

V. CYBERWAR

As a first step, it is important to distinguish cyberwar from cyberwarfare. According to Robinson, cyberwarfare is to be understood as an activity that uses cyberattack with a warfare intent, where cyberwar is more closely related to a state of being.[54] Furthermore, cyberwar can also be characterised as cyber-hostilities recognised as war by the international community and by international law.[55] Warfare is the term used to refer to the tools used to fight a war.[56] Furthermore, the perpetrators of a cyberwar can be nation

[47] Ibid.
[48] HATHAWAY, OONA A., et al., "The law of cyber-attack", *Calif. L. Rev.*, 2012, p. 817.
[49] Ibid.
[50] ROBINSON, MICHAEL, KEVIN JONES, and HELGE JANICKE, "Cyber warfare: Issues and challenges", *Computers & security*, 2015, p.70-94.
[51]LUIJF, ERIC, "Understanding cyber threats and vulnerabilities", *Critical infrastructure protection*, 2012, p. 52-67.
[52] Ibid.
[53]ROBINSON, MICHAEL, KEVIN JONES, and HELGE JANICKE, "Cyber warfare: Issues and challenges", *Computers & security*, 2015, p.70-94.
[54]ROBINSON, MICHAEL, KEVIN JONES, and HELGE JANICKE, "Cyber warfare: Issues and challenges", *Computers & security*, 2015, p.70-94.
[55] BEIDLEMAN, SCOTT W., "Defining and deterring cyber war", *Army War Coll Carlisle Barracks Pa*, 2009, p. 1-32.
[56]ROBINSON, MICHAEL, KEVIN JONES, and HELGE JANICKE, "Cyber warfare: Issues and challenges", *Computers & security*, p. 70-94, 2015.

states,[57] non-state actors[58] or 'private hackers'[59] without personal motivations.[60] What differentiates cyberwar from other types of cyberattacks is the effect that it can have on the target and the purpose of the cyberattack. The effect of cyberwar on their targets is *"physical injury or property damage comparable to a conventional armed attack*".[61]

However, in reality, actual military activities are limited[62] and not regulated by the international instruments that deal with cybersecurity. Indeed, most of the selected instruments do not use the terms cyberwar or cyberwarfare, but do affirm that international law principles apply to cyberspace, thus extending existing rules to cyber situations.[63] For instance, Resolution 45 recognises that the information society should be premised on: *"principles of the Charter of the United Nations, international law and multilateralism, and respecting fully and upholding the Universal Declaration of Human Rights".*[64] In the same sense, the Declaration Strengthening Cyber-Security in the Americas, developed by the OAS, declares a commitment to fighting terrorism by respecting *"the sovereignty of the States and compliance with their obligations under national and international law, including international human rights law, international humanitarian law, and international refugee law."*[65] The recognition that international law applies in cyberspace through the international norms does not imply that there is consensus about how it should be applied. Indeed, the fifth UN Group of Governmental

[57] CORNISH, PAUL, et al., "On cyber warfare", *Chatham House*, London, 2010; BILLO, CHARLES, and WELTON CHANG. "Cyber warfare", *An Analysis of the means and motivations of selected nation states. Dartmouth, ISTS*, 2004; KENNEY, MICHAEL, "Cyber-terrorism in a post-stuxnet world", *Orbis*, 2015, p.111-128; UMA, M., and GANAPATHI PADMAVATHI, "A Survey on Various Cyber Attacks and their Classification", *Int. J. Netw. Secur.*, 2013, p.390-39.

[58]GREATHOUSE, CRAIG B., "Cyber war and strategic thought: Do the classic theorists still matter?", *Cyberspace and International Relations*. Springer, Berlin, Heidelberg, 2014, p.21-40.

[59] KENNEY, MICHAEL, "Cyber-terrorism in a post-stuxnet world", *Orbis*, 2015, p.111-128.

[60] DIPERT, RANDALL R., "The ethics of cyberwarfare", *Journal of Military Ethics*, 2010, p.384-410.

[61] HATHAWAY, OONA A., et al. 'The law of cyber-attack', *Calif. L. Rev.*, 2012, p.817.

[62] DUCHEINE, P. A. L., and PETER BMJ PIJPERS, "The Notion of Cyber Operations", *Amsterdam Law School Research Paper*, 2020, p.2020-09.

[63] INTERNATION TELECOMMUNICATION UNION, "recognizing, c)", *Resolution 45 – Effective coordination of standardization work across study groups in ITU-T and the role of TSAG*, Dubai, 20-29; ORGANIZATION OF AMERICAN STATES, "Reaffirming", *Declaration strengthening cyber-security in the americas*, 7 de March de 2012; ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE, *Decision 1106 - Initial Set of OSCE Confidence-Building Measures To Reduce The Risks Of Conflict Stemming From The Use Of Information And Communication Technologies*, 3 de December de 2016; SHANGHAI COOPERATION ORGANIZATION, "Article 4", *Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization*, 2009.

[64] INTERNATION TELECOMMUNICATION UNION, "recognizing, c)", *Resolution 45 – Effective coordination of standardization work across study groups in ITU-T and the role of TSAG*, Dubai, 20-29.

[65] ORGANIZATION OF AMERICAN STATES, "Reaffirming", *Declaration strengthening cyber-security in the americas*, 07 March 2012.

Experts (GGE) failed to reach a consensus on its final report about specific branches of international law, such as armed conflict, self-defence and countermeasures. Three states were reportedly opposing the adoption of the report: China, Cuba and the Russian Federation. [66]

One year later, UN Resolution nº 73/27, based on Report A/70/174, concluded that international law is applicable to cyberspace, including the principles of sovereign equality, peaceful settlement of international disputes, refraining from the threat or use of force against the territorial integrity or political independence of any State, respect for human rights and fundamental freedoms and non-intervention in the internal affairs of other states. The same Resolution also affirms that the dissemination of false or distorted news, as one of the main threats that could affect the promotion of peace, cooperation and friendly relations among states, can be interpreted as interference in the internal affairs of the states.[67] In this context, member states should abstain from any defamatory campaign, hostile propaganda for the goal of intervening in the internal affairs of other states.[68]

The Resolution was proposed by the Russian Federation in collaboration with 32 other states. A total of 109 member states voted in favor, while 46 voted against it. The majority of the states supporting the resolution were from Africa,[69] Asia[70] South America,[71] Central America,[72] and the Middle East.[73] On the other hand, countries such as France, Italy, the Netherlands, the United Kingdom and the United States voted against it.[74] One year later, a number of the states that supported the Resolution that also are parties to the Shanghai Cooperation Organization (SCO) [75] defined cyberwar as:

[66] DELERUE, FRANÇOIS, *Cyber operations and international law*, Cambridge University Press, 2020.
[67] UNITED NATIONS GENERAL ASSEMBLY, *Resolution 73/27 - Developments in the field of information and telecommunications in the context of international security*, 05 December 2018.
[68] Ibid.
[69] For example, Algeria, Andorra, Burundi, Cabo Verde , Central African Republic, Comoros, Congo, Cote D'ivoire, Democratic Republic Of The Congo, Djibouti, Egypt, Equatorial Guinea, Eritrea, Ethiopia, Gambia, Georgia, Ghana, Guinea, Guinea-Bissau, Kenya, Kuwait, Kyrgyzstan.
[70] For Example, Bangladesh, Bhutan, Brunei Darussalam, Burkina Faso, Cambodia, China, Democratic People's Republic of Korea, India
[71] For example, Argentina, Bolivia, Colombia, Dominican Republic, Ecuador, Guyana, Paraguay, Peru.
[72] For example, Barbados, Belize, Costa Rica, Cuba, El Salvador, Guatemala, Honduras.
[73] For example, Azerbaijan, Bahrein, Iran, Iraq, Jordan, Kazakhstan.
[74] UNITED NATIONS GENERAL ASSEMBLY, *Resolution 73/27 - Developments in the field of information and telecommunications in the context of international security*, 05 December 2018.
[75] The Shanghai Cooperation Organization is an international organization where the members are: The Russia Federation, Republic of Kazakhstan, Kyrgyz Republic, Republic of Uzbekistan, Republic Tajikistan, Republic of India, Islamic Republic of Pakistan, People's Republic of China.

Confrontation between two or more states in the information space with the aim of damaging information systems, processes and resources, critically important and other structures, undermining political, economic and social systems, psychologically manipulating masses of the population to destabilize society and the State, and also forcing the state to take decisions in the interest of the opposing party.[76]

It is possible to infer from this definition that cyberwar can take place in two different situations. First, if there is a conflict between two or more states that resulted in damaging infrastructure. This situation can be compared to the understanding that cyberwar should have a kinetic effect that generates physical injury comparable to a conventional armed attack. The second situation focuses on wrongful interventions in cyberspace that has negative effect on the economic, political and social system of the country, manipulates masses and forces the state to make decisions. This circumstance can be compared to the idea developed in Resolution nº 73/27 where fake news or a defamatory campaign can be considered forms of intervening in the international affairs of the country.

This second part of the definition of cyberwar has been criticised as being a form of justifying censorship on the internet.[77] Indeed, giving power to the state to control information can affect basic citizens' rights such as freedom of expression and access to information. On the other hand, the discussion around the approval of Resolution nº 73/27 can also represent a non-western concern about foreign interference at the national level, where cyberspace is used as a place to spread fake information. As stated throughout this study, there is a conflict between two different views about the role of the state in cyberspace. Nonetheless, the Resolution shows that the conflict goes beyond the dichotomy between Russia/China and Europe/United States as there are also divergences with other regions such as Africa, Asia, South America and Central America. This means that on this specific topic there is a fragmentation of international law where the norms are only applicable regionally or for a few states. In this context, at the regional level, like-minded states tend to go further in the norm-building process.[78] It also means that SCO did not need to push for cyber sovereignty because other countries, with different regime types, share the same fear regarding to the internet being used as a form of external

[76] SHANGHAI COOPERATION ORGANIZATION. "Information War, List of Basic Terms in the Field of International Information Security", *Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization*, 2009.
[77] HATHAWAY, OONA A., et al., "The law of cyber-attack", *Calif. L. Rev.,* 817, 2012.
[78] DELERUE, FRANÇOIS, *Cyber operations and international law*, Cambridge University Press, 2020.

inference in national affairs. This finding is relevant because it demonstrates that there are not two groups (the United States/Europe x China/Russia) with cohesive thoughts but there is a third group of countries that also fear the influence of third states on their national sovereignty.

This is important because it highlights the complexity and singularities of the cybersecurity governance model that cannot be divided only into two main groups: on one side, the Western countries, represented by United States and Europe, and on the other side, Non-Western countries represented by Russia and China. There are other countries with different interests and levels of technological development that are also worried about the external influence of the internet on national affairs. The internet is not as open as it used to be and the group of countries pushing for wider participation in the regulation of the internet regulation is growing. This also means that the polarisation of the internet tends to increase and an international organisation such as the UN GGE is an important forum to facilitate this discussion and to improve consistency in the various understandings of cyberwar.

VI. CYBERCRIME

The internet has not only transformed social relations, but at the same time is also responsible for the appearance of a new type of criminal behavior: cybercrime.[79] Like other cyberthreats, there is no agreement on the definition of cybercrime.[80] Frequently, cybercrime is understood as an extension of existing criminal behavior[81] in which different types of electronic devices are used to break the law.[82] Yet, the tools used to commit cybercrime are electronic devices. For example, Brenner affirms that cybercrime is "*a crime committed on a computer network*".[83] Following this line of thought, Hathaway argues that cybercrime is "*any crime that is facilitated or committed using a computer network or hardware device*". [84] According to the literature, the most frequent

[79]KASTNER, PHILIPP, and FRÉDÉRIC MÉGRET, "International legal dimensions of cybercrime", *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing, 2021.
[80] DELERUE, FRANÇOIS, *Cyber operations and international law*, Cambridge University Press, 2020.
[81]TECHOPEDIA, "*Cyberattack"*, 5 February 2019, <https://www.techopedia.com/definition/24748/cyberattack>; GORDON, SARAH, and RICHARD FORD, "On the definition and classification of cybercrime", *Journal in Computer Virology*, 13-202, 2006; MEHAN, JULIE. "CyberWar, CyberTerror, CyberCrime and CyberActivism: An i-depth guide to the role of standards in the cybersecurity environment", *IT Governance Publishing*, 2014.
[82] MCQUADE III, SAMUEL C., "Encyclopedia of cybercrime", *ABC-CLIO*, 2008.
[83] BRENNER, SUSAN W. "Cybercrime, cyberterrorism and cyberwarfare", *Revue internationale de droit penal*, 2006, p.453-471.
[84] HATHAWAY, OONA A., et al., "The law of cyber-attack", *Calif. L. Rev.*, 2012, p.817.

electronics devices used to commit cybercrimes are the computer[85] network[86], information systems[87], telephones and equipment.[88] The purpose of cybercrime is violating the law.[89] The consequences of cybercrime are profit[90] and personal gain.[91] Cybercrime is an important pillar for cybersecurity because criminals take advantage of the cyber environment which has the power to affect different jurisdictions on a global level.[92] Cybercrime, like the other cyberthreats, has a cross-border dimension where action can involve users or entities located abroad. Consequently, this phenomenon creates challenges because criminal law is primarily national law and is enforced by national authorities, at the same time and this type of crime necessitates law enforcement authorities and investigation in different countries.[93]

Several international norms regulate this type of cyberthreat. The most important instrument is the Convention on Cybercrime of the Council of Europe (Budapest Convention) which entered in force in 2004. This treaty aims to create a common criminal policy while protecting society against cybercrime.[94] It covers criminalisation, mutual legal assistance and safeguards in criminal investigations, which resulted in the most

[85] FAGA, HEMEN PHILIP, "The implications of transnational cyber threats in international humanitarian law: analysing the distinction between cybercrime, cyber attack, and cyber warfare in the 21st century", *Baltic Journal of Law & Politics*, vol. 10, 2017, p. 35-62; CHAWKI, MOHAMED, et al., "Cybercrime, digital forensics and jurisdiction", *Springer*, 2015, vol. 593; WILSON, CLAY, *Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress*, Library of congress Washington DC Congressional Research Service, 2008; HATHAWAY, OONA A., et al., "The law of cyber-attack", *Calif. L. Rev.*, 2012, p.817; SPEER, DAVID L., "Redefining borders: The challenges of cybercrime", *Crime, law and social change*, 2000, p. 259-273; MCQUADE III, SAMUEL C., ed., *Encyclopedia of cybercrime*, ABC-CLIO, 2008.

[86] HATHAWAY, OONA A., et al., "The law of cyber-attack", *Calif. L. Rev.*, 2012, p.817.

[87] SABILLON, REGNER, et al., "Cybercriminals, cyberattacks and cybercrime", *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, 2016.

[88]SPEER, DAVID L., "Redefining borders: The challenges of cybercrime", *Crime, law and social change*, 2000, p. 259-273.

[89] FAGA, HEMEN PHILIP, "The implications of transnational cyber threats in international humanitarian law: analysing the distinction between cybercrime, cyber attack, and cyber warfare in the 21st century", *Baltic Journal of Law & Politics*, vol. 10, 2017, p. 35-62; ROBINSON, MICHAEL and JONES, KEVIN and JANICKE, HELGE, "Cyber warfare: Issues and challenges", *Computers & security*, 2015, p. 70-94: MCQUADE, SAMUEL C., "Understanding and managing cybercrime", *Pearson/Allyn and Bacon* Boston, 2006; Speer, David L., "Redefining borders: The challenges of cybercrime", *Crime, law and social change*, 2000, p. 259-273.

[90] GREATHOUSE, CRAIG B., "Cyber war and strategic thought: Do the classic theorists still matter?", *Cyberspace and International Relations*, Springer, Berlin, 2014, p.21-40; STRUNK, DANIEL, et al., *American Cyber Insecurity: The growing danger of cyber attacks*, Duke University, Durham, 2014.

[91] ROBINSON, MICHAEL and JONES, KEVIN and JANICKE, HELGE, "Cyber warfare: Issues and challenges", *Computers & security*, 2015, p.70-94.

[92] EUROPEAN COMISSION, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, 2013.

[93] BRUNHÖBER, BEATRICE, "Criminal Law of Global Digitality: Characteristics and Critique of Cybercrime Law", *The Law of Global Digitality*. Routledge, 2022, p.223-249.

[94] COUNCIL OF EUROPE, *Convention on Cybercrime (ETS No. 185)*, 01 de 07 de 2004.

comprehensive and most widely accepted existing international standard on fighting cybercrime.[95] Currently, 44 Members of the Council of Europe and 21 non-members have ratified it. Countries such as China, Brazil and the Russian Federation are still not parties to the Convention.

The Budapest Convention is acknowledged by the European Union, the United Nations, the OECD and the Paris Call as a reference to combat cybercrime.[96] Arguably the most controversial issue of the Convention is the application of Article 32 (b), dealing with the transborder access to electronic evidence.[97] There is no consensus on the limits of the interpretation of Article 32, especially regarding the extraterritorial power that enforcement authorities would have to order and collect evidence for purposes of criminal investigations.[98] Countries like the Russian Federation argued that article 32 (b) is a way of jeopardising the principle of state sovereignty.[99] Article 32 authorises two possibilities regarding transborder searches. The first allows access to data located extraterritorially without the authorisation of another party if it is publicly available (open source).[100] The second, and more controversial, possibility allows a party to *'access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system'.*[101]

In other words, this provision allows, for example, law enforcement in one country to access data stored in another country without notifying the national authorities in that country. For example, the owner of data stored in one country can allow access to that data to local enforcement. Nonetheless, in a context where private companies are responsible for storage and collect large amounts of data, the consent of the lawful authority can be given by multinational companies like Google or Facebook.[102]

---

[95] TROPINA, TATIANA, *Cybercrime: Setting international standards*, Routledge Handbook of International Cybersecurity, Routledge, 148-160, 2020.
[96] ORGANISATION OF AMERICAN STATES (OECD), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, Paris, 2015.
[97] JAHN, JESSICA, "Canada´s Position at the UN Cybercrime Treaty Negotiations", <https://icclr.org/2022/03/02/canadas-position-at-the-un-cybercrime-treaty-negotiations/>.
[98] VELASCO, CRISTOS, HÖRNLE, JULIA, and OSULA, ANNA-MARIA, "Global Views on Internet Jurisdiction and Trans-border Access", *Data Protection on the Move*. Springer, 465-476, Dordrecht, 2016.
[99] TROPINA, TATIANA, *Cybercrime: Setting international standards*, Routledge Handbook of International Cybersecurity. Routledge, 148-160, 2020.
[100] COUNCIL OF EUROPE, "Article 32, (a)", *Convention on Cybercrime (ETS No. 185)*, 01 07 2004.
[101] Id at Article 32, (a), *Convention on Cybercrime (ETS No. 185)*, 01 07 2004.
[102] CLOUGH, JONATHAN, "A world of difference: The Budapest convention on cybercrime and the challenges of harmonization", *Monash University Law Review*, 2014, p. 698-736.

Even though the discussion about the application of Article 32 is relevant for understanding the discussions about the application of the Budapest Convention, the aim of this paper is not to analyse the criminal offences in the Budapest Convention in depth, but to examine the consistency between various cybercrime norms. Within the broader context of our project, we selected three instruments: The Arab Convention on Combating Information Technology Offences, the African Union Convention on Cyber Security and Personal Data (AU Convention), and Directive n° 2013/40 created by the European Union.

The purpose of the Arab Convention is to enhance cooperation in combating information technology offences to protect security.[103] In 2011, the African Union Convention on cybersecurity and personal was adopted by the twenty-third ordinary session of the assembly on 27 of June 2014. The instrument was signed by only 14 out of 55 countries that are part of the African Union and ratified by five members (Ghana, Guinea, Mauritius, Namibia and Senegal).[104] In order for the norm to come into force it must be signed and ratified by a minimum of 15 states. This implies that the norm is not yet in force. The convention is divided into three parts: (1) electronic transactions, (2) personal data protection and (3) cybersecurity and cybercrime. Even though the norm is not in force it was included in our analysis because we considered that it is important to include the perspective of the African Union in our analysis and the norm may enter into force in the future. In 2013 EU Directive nº 2013/40 was released. This Directive replaced Framework Decision 2005/222/JHA on attacks against information systems. The former Decision aimed to relate criminal law with cyberattacks and intended to be constituent with the CoE Convention.[105] However, there are some differences between the Convention and the Directive. The Directive focuses more on procedure law than the Budapest Convention. In addition, the AU Convention did not contain a mechanism for cooperation then the Council of Europe Convention.[106]

Our comparison of the chosen instruments is based on the structure of the Budapest Convention as the other instruments have a similar approach. The Convention has three

[103] THE LEAGUE OF ARAB STATES, "Article 3", *Arab Convention on Combating Information Technology*. 15 Feb 2012.
[104] AFRICAN UNION, List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection
[105] BUSSOLATI, NICOLÒ, "Harmonisation of cybercrime law: Past solutions, present tensions, and future challenges", 2020.
[106] KASTNER, PHILIPP, and MÉGRET, FRÉDÉRIC, "International legal dimensions of cybercrime", *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing, 2021.

pillars: substantive law pillar, criminal procedure and mutual legal assistance.[107] The substantive law is divided into four offences: Offences against the confidentiality, integrity and availability of computer data and systems (illegal access, illegal interception, data interception, system interference and misuse of devices); computer-related offences (computer-related forgery and computer-related fraud); content-related offences (offences related to child pornography, xenophobic nature, hate speech) and copyright-related offences. We observe that, overall, the norms that deal with cybercrime are consistent because the structure is similar and the content of the criminal offence is close. We will shortly mention the various offences.

Computer-related offences are the ones that address the manipulation of computer systems or data.[108] This criminal offence is always intending to produce a consequence that is detrimental to lawful rights, and the victim is deprived of something of value.[109] In the Budapest Convention 'computer-related fraud' is defined as *"the causing of a loss of property to another person by: b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person."*[110] In the Arab Convention on Combating Information Technology the offence of fraud is described as *"Intentionally and unlawfully causing harm to beneficiaries and users with the aim of committing fraud to illicitly realize interests and benefits to the perpetrator or a third party, through: 2- interfering with the functioning of the operating systems and communication systems, or attempting to disrupt or change them."*[111] Finally, Article 29,1, c) of the African Union Convention (AU) reads: *"Remain or attempt to remain fraudently in part or all of a computer system"*.[112] The main difference between the norms is to be found in the motives of the attacker. In the Budapest Convention, the motive of the attacker is to gain economic benefits. Meanwhile, for the Arab Convention, the purpose of the criminal offences is broader and includes 'interest and benefits'. This means that for the Arab Convention the

[107] TROPINA, TATIANA, *Cybercrime: Setting international standards*, Routledge Handbook of International Cybersecurity. Routledge, 148-160, 2020.
[108] KASTNER, PHILIPP, and MÉGRET, FRÉDÉRIC, "International legal dimensions of cybercrime", *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing, 2021.
[109] VASIU, LUCIAN, and VASIU, IOANA, "Dissecting computer fraud: from definitional issues to a taxonomy", *37th Annual Hawaii International Conference on System Sciences*, 2004.
[110] COUNCIL OF EUROPE, "Article 5", *Convention on Cybercrime (ETS No. 185)*, 01 07 2004.
[111] Id at "Article 11", *Convention on Cybercrime (ETS No. 185)*, 01 07 2004.
[112] Id at "Article 29, 1, c)", *Convention on Cybercrime (ETS No. 185)*, 01 de 07 de 2004; African Union. "Article 29, 1, c)", *African Union Convention on Cyber Security and Personal Data Protection*, 27 June 2014.

attacker can present other motives than economic ones. In the case of the African Convention, no motives for the attacker are described and is not clear what the term "remain" means. For example, how much time must the offender be in the computer system to constitute an offence? The AU Convention is criticised for being vague and it can be interpreted as containing aspirational principles that require further regulation to make the norms more concrete. [113]

Regarding the criminal offence of 'child pornography', the content is related to the Convention of Cybercrime and the African Convention. According to the Budapest Convention, the term 'child pornography' comprises pornographic material that includes a minor, a person appearing as a minor, or images representing a minor engaging in explicit sexual conduct.[114] In contrast, Article 12 of the Arab Convention establishes that not only is child pornography a crime, but pornography, in general, constitutes a criminal offence. This can be explained by the fact that criminal offences are shaped by cultural conceptions of the national state.

Furthermore, most procedural powers provided for by the Budapest Convention are missing in the AU Convention or are only vaguely defined and lack aspects related to criminal justice cooperation between parties. This raises concerns that the African states are likely to implement the procedures in a different manner and, consequently, could hinder the harmonisation of cybercrime at the domestic level and enable cooperation.[115] In contrast, the Arab Convention contains similar provisions, procedural powers and forms of international cooperation as those in the Budapest Convention.

As we have seen, there is thus a minimum common agreement between the instruments in which criminal offences are relevant. Nonetheless, there are still divergences. While we value the differences and complexity as they allow for specific applications in different contexts, we would also agree that divergences can also lead to clusters that are not well suited for a threat with a global nature such as cybercrime.[116]

[113] JAMIL, ZAHID, "Comparative analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime", *Council of Europe*, 2016.
[114] COUNCIL OF EUROPE, "Article 9,2", *Convention on Cybercrime (ETS No. 185)*, 01 07 2004.
[115] JAMIL, ZAHID, "Comparative analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime", *Council of Europe*, 2016.
[116] CLOUGH, JONATHAN, "A world of difference: The Budapest convention on cybercrime and the challenges of harmonization", *Monash University Law Review*, 2014, p.698-736.

The question thus remains how to harmonise cybercrimes offences if the national states and, in our case organisations, have different cultural perspectives.[117] The answer to this question is currently being discussed in the United Nation proposal for the international Convention on Cybercrime. We have not yet been able to fully include this instrument because the first meeting was held in 2022. In December 2019, the UN General Assembly adopted the nº 74/247 on "Countering the use of information and communications technologies for criminal purposes", launching an Ad Hoc intergovernmental committee with the aim of launching a process towards elaborating a cybercrime international convention.[118] According to Resolution 75/282, the process of elaborating the UN convention should take into account existing international instruments, national and regional norms.[119]

In conclusion, the Budapest Convention is considered the most important instrument in this regard and it serves as a foundation for other international criminal law regulations that largely coincide in terms of definitions. Despite this, we found two inconsistencies related to specific criminal offences. The first inconsistency is related to the criminal offence that deals with fraudulent interference in a computer system. The second relates to the criminalisation of pornography. Other points that hinder cooperation between states were found in the AU Convention which contains vague procedural provisions and lacks aspects related to criminal justice cooperation.

VII. CONCLUSION

This paper had a modest aim. Within the framework of a larger study on the governance and regulation of cybersecurity, our goal was to find out whether in the key instruments, that we selected on the basis of their relevance for the topic at hand, we could find consistency in the way the various dimensions of cybersecurity are regulated at the international level. We focused on five types of cyberthreats: cyberattack, cyberwar, cybercrime, cyberespionage and cyberterrorism. Our findings revealed that the European Union and the United Nations have a similar understanding of the notion of cyberattack where the context of the event, the nature and the consequences of the attack are

[117] BRUNHÖBER, BEATRICE, "Criminal Law of Global Digitality: Characteristics and Critique of Cybercrime Law", *The Law of Global Digitality*, Routledge, 2022, p.223-249.
[118] GENERAL ASSEMBLY OF THE UNITED NATIONS, *Resolutions 74/28 - Advancing responsible State behaviour in cyberspace in the context of international security*, 18 December 2019.
[119] GENERAL ASSEMBLY OF THE UNITED NATIONS, *Resolution 75/282- Countering the use of information and communications technologies for criminal purposes*, 26 May 2021.

concerned. Regarding cyberterrorism, there are only a few instruments that define this type of cyberthreat, including the Arab Convention and the Shanghai Cooperation Organization, and no major differences seem to stand in the way of a common understanding. Regarding cyberwar, United Nations Resolution n° 73/27 and the Shanghai Cooperation Organisation (SCO) both relate cyberwar to the dissemination of fake news. Critics fear that this definition of cyberwar can be a form of justifying censorship of the internet. On the other hand, there is a concern by non-western countries about foreign interference at the national level, where cyberspace is used as a place to spread fake information. This means that on this specific topic there is indeed a fragmentation of applicable legal norms, but that this fragmentation is related to regional diversity. Indeed, at the regional level, like-minded states tend to go further in the norm-building process, which may lead to a certain fragmentation at the global level.[120] To improve cybersecurity at the international level there is a need to enhance universal cooperation and the UN GGE can be the forum to take the lead in improving this situation. Finally, cybercrime is the cyberthreat that is most frequently cited in the various instruments we studied. The cybercrime instruments follow the same structure, but we found specific inconsistencies regarding two criminal offences. The main inconsistencies relate to fraudulent interference in the function of a system. For the Budapest Convention, the objective of this criminal offence is a loss of property and the purpose of the attacker is to gain economic benefit. The Arab Convention, on the other hand, does not specify the objective of the attack and the purpose of the attacker is more generally said to be related to 'interest and benefits'. Finally, the African Union did not specify any intended result or purpose of the attacker. In an environment where cyberattacks are global, the different understandings of cybercrime not only cause legal uncertainty and prevent cooperation, but may also make it easier for perpetrators to seek gaps in the normative system.

Overall, our findings suggest that, despite the quite fragmented regulatory systems around the world, there is to a very large extent agreement on the basic notions and definitions. This offers a good starting point for the ongoing debates on a further harmonisation of the global norms on cybersecurity, such as in the case of cybercrime.

[120] DELERUE, FRANÇOIS, "Reinterpretation or Contestation of International Law in Cyberspace?" *Israel Law Review*, 2019, p. 295-326.

VIII. BIBLIOGRAPHY

AFRICAN UNION. *African Union Convention on Cyber Security and Personal Data Protection*. 27 de June de 2014.

ARMY TRAINING AND DOCTRINE COMMAND FORTLEAVENWORTH KS DEPUTY CHIEF OF STAFF FOR INTELLIGENCE, *DCSINT Handbook No 1.02*, 2005.

EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA), <https://www.enisa.europa.eu>.

BEIDLEMAN, SCOTT W., "Defining and deterring cyber war", *Army War Coll Carlisle Barracks Pa*, 2009, p. 1-32.

BOTEK, ADAM, *European Union establishes a sanction regime for cyber-attack*, <https://ccdcoe.org/incyder-articles/european-union-establishes-a-sanction-regime-for-cyber-attacks/>.

BRENNER, SUSAN W., "Cybercrime, cyberterrorism and cyberwarfare", *Revue internationale de droit penal,* v.77, n.3, 2006, p. 453-471.

BRUNHÖBER, BEATRICE, "Criminal Law of Global Digitality: Characteristics and Critique of Cybercrime Law", *The Law of Global Digitality*. Routledge, 2022, p.223-249.

BUCHAN, RUSSELL, *Cyber espionage and international law*, Research handbook on international law and cyberspace, Edward Elgar Publishing, 2015.

BUSSOLATI, NICOLÒ, "Harmonisation of cybercrime law: Past solutions, present tensions, and future challenges", 2020.

CHAWKI, MOHAMED, et al., "Cybercrime, digital forensics and jurisdiction", vol. 593, *Springer*, 2015.

CLOUGH, JONATHAN, "A world of difference: The Budapest convention on cybercrime and the challenges of harmonization", *Monash University Law Review*, 2014, p. 698-736.

CONWAY, MAURA, "Reality bytes: cyberterrorism and terrorist 'use' of the Internet", *First Monday*, v. 7, n. 11, 2002, p. 1-17.

CORNISH, PAUL, "Cyber security and politically, socially and religiously motivated cyber attacks", *European Parliament*, Brussels, 2009.

COUNCIL OF EUROPE, *Convention on Cybercrime (ETS No. 185)*, 01 de 07 de 2004.

DELERUE, FRANÇOIS, "Reinterpretation or Contestation of International Law in Cyberspace?" *Israel Law Review,* 2019, p. 295-326.

DENNING, D., "A view of cyberterrorism 5 years later", *Internet security: Hacking, counterhacking, and society,* p. 123, 2007.

DE SANTANNA, JOSÉ JAIR CARDOSO, *DDoS-as-a-Service: investigating booter websites*, Enschede, 2017.

DIPERT, RANDALL R, "The ethics of cyberwarfare", *Journal of Military Ethics*, 2010, p. 384-410.

DUCHEINE, P. A. L., and PETER BMJ PIJPERS, "The Notion of Cyber Operations", *Amsterdam Law School Research Paper,* 2020, p.2020-09.

EUROPEN UNION, *Council Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States*, 17 May 2019.

EUROPEAN UNION, *European Parliament resolution of 12 September 2013 on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013/2606(RSP)),* 12 September 2013.

FAGA, HEMEN PHILIP, "The implications of transnational cyber threats in international humanitarian law: analysing the distinction between cybercrime, cyber attack, and cyber warfare in the 21st century", *Baltic Journal of Law & Politics*, vol. 10, 2017, p. 35-62.

GENERAL ASSEMBLY OF THE UNITED NATIONS, *Resolutions 74/28 - Advancing responsible State behaviour in cyberspace in the context of international security,* 18 December 2019.

GENERAL ASSEMBLY OF THE UNITED NATIONS, *Resolution 75/282- Countering the use of information and communications technologies for criminal purposes*, 26 May 2021.

GENERAL ASSEMBLY OF THE UNITED NATIONS, *Resolution 73/27 - Developments in the field of information and telecommunications in the context of international security*, 05 December 2018.

GENERAL ASSEMBLY OF THE UNITED NATIONS, *Resolution nº 58/199 - Creation of a global culture of cybersecurity and the protection of critical information infrastructures*, 30 January 2004.

GREATHOUSE, CRAIG B., “Cyber war and strategic thought: Do the classic theorists still matter?”, *Cyberspace and International Relations*. Springer, Berlin, Heidelberg, 2014, p.21 - 40.

GORDON, SARAH, and RICHARD FORD, “On the definition and classification of cybercrime”, *Journal in Computer Virology,* 13-202, 2006

HANSMAN, SIMON, and HUNT, RAY, “A taxonomy of network and computer attacks”, *Computers & Security,* 2005, p. 31-43.

HATHAWAY, OONA A., et al., “The law of cyber-attack”, *Calif. L. Rev.,* 2012, p. 817.

INTERNATIONAL TELECOMMUNICATION UNION, *Resolution 50,* 25 October – 3 November 2016.

INTERNATION TELECOMMUNICATION UNION, *Resolution 45 – Effective coordination of standardization work across study groups in ITU-T and the role of TSAG,* Dubai, 20-29.

JAMIL, ZAHID, “Comparative analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime”, *Council of Europe,* 2016.

JAHN, JESSICA, "Canada´s Position at the UN Cybercrime Treaty Negotiations", <https://icclr.org/2022/03/02/canadas-position-at-the-un-cybercrime-treaty-negotiations/>.

KASTNER, PHILIPP, and FRÉDÉRIC MÉGRET, “International legal dimensions of cybercrime”, *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing, 2021.

KENNEY, MICHAEL, “Cyber-terrorism in a post-stuxnet world”, *Orbis, vol.* 59, n.1, 2015, p. 111-128.

LIN, HERBERT, “Lifting the veil on cyber offense”, *IEEE Security & Privacy*, 2009, p.15-21.

LUIJF, ERIC, “Understanding cyber threats and vulnerabilities”, *Critical infrastructure protection,* 2012, p. 52-67.

MCQUADE III, SAMUEL C., “Encyclopedia of cybercrime”, *ABC-CLIO,* 2008.

MEHAN, JULIE. “CyberWar, CyberTerror, CyberCrime and CyberActivism: An i-depth guide to the role of standards in the cybersecurity environment”, *IT Governance Publishing,* 2014.

MIADZVETSKAYA, YULIYA, “Challenges of the Cyber Sanctions Regime Under Common Foreign and Security Policy (CFSP)”, *Anton Vedder, Jessica Schroers, Charlotte Ducuing, Peggy Valcke, KU Leuven Centre for IT & IP Law Series*, 2019.

NYE JR, JOSEPH S., *Cyber power*. Harvard Univ Cambridge Ma Belfer Center for Science and International Affairs, 2010.

ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE, *Decision 1106 - Initial Set of OSCE Confidence-Building Measures To Reduce The Risks Of Conflict Stemming From The Use Of Information And Communication Technologies,* 3 December 2016.

ORGANIZATION OF AMERICAN STATES, *Declaration strengthening cyber-security in the americas,* 7 March 2012.

ORGANISATION OF AMERICAN STATES (OECD), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document,* Paris, 2015.

PATTISON, JAMES, “From defence to offence: The ethics of private cybersecurity”, *European Journal of International Security,* vol. 5, 2020, p. 233-254.

PERNICE, INGOLF, “Cybersecurity governance: Making cyberspace a safer place”, *HIIG Discussion Paper Series,* vol. 3, 2017, p. 1-28.

ROBINSON, MICHAEL, KEVIN JONES, and HELGE JANICKE, “Cyber warfare: Issues and challenges”, *Computers & security,* 2015, p.70-94.

SABILLON, REGNER, et al., “Cybercriminals, cyberattacks and cybercrime”, *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF),* 2016.

SPEER, DAVID L., “Redefining borders: The challenges of cybercrime”, *Crime, law and social change*, 2000, p. 259-273.

SHACKELFORD, SCOTT J., “Toward cyberpeace: Managing cyberattacks through polycentric governance” *Am. UL Rev.*, vol. 62, 2012, p. 1273.

SHANGHAI COOPERATION ORGANIZATION, *Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization*, 2009.

SAMARASEKERA, UDANI, *Cyber risks to Ukrainian and other health systems*, 30 March 2022, <https://www.thelancet.com/journals/landig/article/PIIS2589-7500(22)00064-4/fulltext>.

SPEER, DAVID L., "Redefining borders: The challenges of cybercrime", *Crime, law and social change*, 2000, p. 259-273.

STRUNK, DANIEL, et al., "American Cyber Insecurity: The growing danger of cyber attacks", *Duke University*, Durham, 2014.

TECH ACCORD, *Cybersecurity Tech Accord. Protecting Users and Customers Everywhere*, 2018.

TECHOPEDIA, <https://www.techopedia.com/definition/24748/cyberattack>.

THE LEAGUE OF ARAB STATES, *Arab Convention on Combating Information Technology*, 15 Feb 2012.

TROPINA, TATIANA, *Cybercrime: Setting international standards*, Routledge Handbook of International Cybersecurity, Routledge, p.148-160, 2020.

UMA, M., AND GANAPATHI PADMAVATHI, "A Survey on Various Cyber Attacks and their Classification", *Int. J. Netw. Secur.*, 2013, p. 390-396.

VASIU, LUCIAN, and VASIU, IOANA, "Dissecting computer fraud: from definitional issues to a taxonomy", *37th Annual Hawaii International Conference on System Sciences*, 2004.

VELASCO, CRISTOS, HÖRNLE, JULIA, and OSULA, ANNA-MARIA, "Global Views on Internet Jurisdiction and Trans-border Access", *Data Protection on the Move*. Springer, 465-476, Dordrecht, 2016.

WARREN, M. J., "Terrorism and the Internet", *Cyber warfare and cyber terrorism*. IGI Global, 2007, p.42-49.

WILSON, CLAY, *Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress*, Library of congress Washington DC Congressional Research Service, 2008.