



SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

Spoke 8 UniBO

EcoCyber

Risk management for future cyber-physical ecosystems

WP4 - Deliverable 4.2.1

GLOBAL CYBERSECURITY GOVERNANCE:
MAIN OPEN ISSUES

15-12-2023

Editor

Giampiero Giacomello (UNIBO)

Contributors

Giulia Gabrielli (UNIMI)

Giampiero Giacomello (UNIBO)

Table of contents

Editor	1
Contributors	1
Table of contents	2
Abstract	3
PART A - International legal framework and policies (UNIMI)	4
1. The Cybersecurity Diplomatic Initiatives within the United Nations	6
1.1 The UN Group of Governmental Experts (UN GGE)	6
1.2 The UN Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG)	12
1.2.1 The OEWG 2019/2020	12
1.2.2 The OEWG 2021/2025	13
1.3 Future processes: The Programme of Action (PoA) for Advancing Responsible State Behaviour in Cyberspace	14
2. The Role for the EU and EU Member States within UN Processes devoted to Cyber Issues	15
3. The Framework of Responsible State Behaviour in Cyberspace	19
3.1 Norms, rules and principles for the responsible behaviour of States	20
3.2 Main Open Issues	22
Part B – Data processing for international policies: empirical perspective (UNIBO)	26
1 The issue of Data Quality for policy decisions.	26
1.1 Introduction	26
1.2 A Glance at the Various Actors	31
1.3 Examples Data collection and structures	34
2 Possible Alternative: Synthetic Data?	40
3 Future Directions of the Research	43
3.1 Where we are now	43
3.2 Where We Go From Here	44

Abstract

The increasing developments in information and communications technologies (ICTs) and the growing dependence of both States and the private sector on digital technologies have raised fundamental questions on the risks and consequences that they may entail. The malicious use of ICTs by States and non-State actors has the potential to undermine international security and stability. In this context, one of the primary challenges posed by cyberspace is the absence of a homogenous legal framework capable of regulating and countering the malicious use of ICTs, with potentially devastating consequences for international peace and security, economic growth, and the full enjoyment of human rights and fundamental freedoms.

In light of these concerns, **Part A** will discuss the international legal framework and policies discussed within the United Nations (UN), where the risks and threats associated with the malicious use of ICTs have been the subject of intense debate for nearly two decades. In particular, the cyber negotiations undertaken within the UN Group of Governmental Experts (GGE) and the UN Open-Ended Group (OEWG) will be addressed in section 1, with a focus on international law and the norms for responsible State behavior, as well as future processes. Section 2 will briefly discuss the role of the European Union (EU) and its Member States within these mechanisms. Section 3 will analyze the framework of responsible State behavior established so far within the UN processes, and the legal nature of the voluntary, non-binding norms, rules, and principles for the ICT environment.

The **Part B** of Deliverable D.4.2.1 will focus, through an empirical study, on the critical issue of quality, relevance, and consistency of data that is being used to develop national and international cybersecurity policy solutions. Specifically, the research introduces a quantitative approach to examining 'cyber power', concentrating on both state and non-state actors (Section 1). The methodology entails collecting data from diverse databases, constructing a comprehensive dataset spanning from 2000 to 2023, and employing quantitative analysis to comprehend cyber-attacks and power dynamics. To overcome limitations related to data availability and quality, Section 2 suggests use of synthetic data as a pivotal alternative. Section 3, finally, explores future directions of the research.

PART A - International legal framework and policies (UNIMI)

In recent decades, the increased development of cyberspace has risen to prominence at an international level. Information and Communication Technologies (ICTs) undoubtedly provide an array of opportunities in terms of social and economic development. At the same time, the growth of alarming trends involving incidents caused by the malicious use of ICTs by States and non-State actors has raised concerns due to the risks they may represent for the international peace and security, especially when these are used for criminal or terrorist purposes.

In absence of a homogenous legal and policy framework to regulate and contrast malicious use of ICTs, the discussion on the adequacy and possible adaptation of the traditional framework of public international law norms and principles in relation to cyber activities has gained momentum at an international, regional, and national level. At a regional level, efforts in normative development to respond to cyber threats have been developed for instance within the Organization for Security and Co-operation in Europe (OSCE),¹ the ASEAN Regional Forum,² the Organization of American States (OAS),³ the African Union (AU),⁴ and the European Union (EU).⁵ Other instances include State-led initiatives including the Paris Call for Trust and Security in Cyberspace,⁶ and various non-State-driven initiatives, including by Microsoft⁷ and the Global Commission on the Stability of Cyberspace (GCSC).⁸

However, the main avenue for the normative development regarding cyberspace and cybersecurity in terms of relevance and participation are the processes undertaken within the United Nations (UN) namely the Group of Governmental Experts (GGE) and the Open-

¹ 'Cyber/ICT Security' available at <<https://www.osce.org/secretariat/cyber-ict-security>>.

² ASEAN Regional Forum Experts and Eminent Persons (ARF/EEP), Recommendations for ARF Initiatives on Promoting Cyber Security (6 March 2018), available at <https://aseanregionalforum.asean.org/wp-content/uploads/2019/01/ANNEX-3_Report-of-the-Working-Group-on-ARF-Initiatives-on-Promoting-Cyber-Security-12th-ARF-EEPs.pdf>.

³ 'Cybersecurity program', available at <<https://www.oas.org/en/sms/cicte/prog-cybersecurity.asp>>.

⁴ African Union's Convention on Cyber Security and Personal Data Protection, entered into force June 8, 2023.

⁵ See section 2.

⁶ Paris Call for Trust and Security in Cyberspace, available at <<https://pariscall.international/en/principles>>.

⁷ A Digital Geneva Convention to protect cyberspace, Microsoft Policy Papers, available at: <<https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH>>.

⁸ Global Commission on the Stability of Cyberspace (GCSC), *Promoting Stability in Cyberspace to Build Peace and Prosperity*, available at: <<https://hcsc.nl/global-commission-on-the-stability-of-cyberspace-homepage/>>.

Ended Working Group (OEWG). These mechanisms have represented the main “organizational platform” for States to negotiate and develop cyber norms, discuss the responsible behaviour of States in cyberspace and have set the global agenda regarding cybersecurity.⁹

The negotiations undertaken within the UN process that were held so far have been instrumental in the affirmation of the applicability of international law norms and principles to ICTs and ICT-related conducts and that these do not occur in a legal vacuum. However, if said applicability appears to be quite uncontested, how the specific norms of international law apply to new technologies is still the object of debate, within these processes and in other fora.

The European Union (EU) and EU Member States have played an important role in the different iterations of the two processes, as well as in framing future discussions regarding information security within the UN, both individually and collectively.

In this context, the term “cyberspace” refers to the virtual environment that includes the Internet, together with computer systems, telecommunication networks, whether they are connected to the Internet or not, and embedded processors and controllers.¹⁰ “Cyber activities” are intended to encompass all those activities that involve the use of computer networks, including the internet.¹¹ “Cybersecurity” has been defined by the International Telecommunication Union (ITU) as “the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets”, which include “connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment”.¹²

⁹ Martha Finnemore, Kathryn Sikkink, ‘International norm dynamics and political change’ (1998) 52 International Organization 887.

¹⁰ Department of Defence Dictionary of Military and Associated Terms (2010) (Joint Publication 1-02), p. 58 https://fas.org/irp/doddir/dod/jp1_02.pdf (“A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers”).

¹¹ Institut de Droit International, Report of the 8th Commission on ‘The Applicability of International Law to Cyber Activities’ (2023) available at <www.idi-iil.org/en/publications/lapplicabilite-du-droit-international-aux-cyber-activites/>.

¹² UN ITU-T X.1205 (04/2008), “Overview of Cyber-security”, p. 2.

1. The Cybersecurity Diplomatic Initiatives within the United Nations

The discussion on information security within the UN, including the consequences of the progress of cyber capabilities and their possible misuse, began with the adoption by the UN General Assembly (UNGA) of Resolution 53/70,¹³ on the proposal of the Russian Federation. Since then, the UNGA included the item “Developments in the field of information and telecommunications in the context of international security” in its agenda for the first time. The negotiations specifically concerning the misuse of ICTs “for purposes that are inconsistent with the objectives of maintaining international stability and security” and possible measures to “enhance the security of global information and telecommunications systems”¹⁴ have been undertaken within the Disarmament and International Security Committee (First Committee).

Since the beginning of the negotiations, three are the main UN cybersecurity diplomatic initiatives under consideration: i.e. the Group of Governmental Experts (GGE), the Open-Ended Working Group (OEWG), and the future Programme of Action to advance responsible State behaviour in the use of information and communications technologies in the context of international security (Cyber PoA).

1.1 The UN Group of Governmental Experts (UN GGE)

In 2003, based on a recommendation of the First Committee,¹⁵ the UNGA requested the UN Secretary-General (UNSG) “with the assistance of a group of governmental experts, to be established in 2004” to undertake a study and to “submit a report on [its] outcome” to the subsequent session of the UNGA.¹⁶

Hence, in 2004, the first Group of Governmental Experts (GGE) was established with the mandate to study “existing and potential threats in the sphere of information security and possible cooperative measures to address them” and the “examination of relevant international concepts aimed at strengthening the security of global information and telecommunications systems” to be included in a submitted report to the UNGA.¹⁷

¹³ United Nations General Assembly Res 53/70 (4 January 1999) UN Doc A/RES/53/70.

¹⁴ Ibid.

¹⁵ UNGA Report of the First Committee (18 November 1998) UN Doc A/53/576.

¹⁶ UNGA Res 58/32 (18 December 2003) UN Doc A/RES/58/32.

¹⁷ UNGA Res 58/32 (18 December 2003) UN Doc A/RES/58/32.

Six GGEs were convened between 2004 and 2019: 2004/2005; 2009/2010; 2012/2013; 2014/2015; 2016/2017; 2019/2021. Four of them achieved an agreement and adopted a consensus report (GGE 2010, GGE 2013, GGE 2015, and GGE 2021). The UNGA resolutions normally detail the Groups' mandate, which largely serves as a workplan. The size and composition of each Group are agreed within the First Committee based on political and budgetary considerations.¹⁸ The size of the GGs has been extended from 15 Member States in 2004/2005, 2009/2010 and 2012/2013, 20 in 2014/2015, and 25 in 2016/2017 and 2019/2021. The GGE members are appointed by the UNSG on the basis of equitable geographical distribution, with the permanent members of the UN Security Council (UNSC) traditionally seating as ex officio members.

The first UN GGE failed in reaching an agreement and did not result in a consensus report. This failure is partly to be attributed to the geopolitical context,¹⁹ and to diverging views on the characterization of the exploitation of ICTs for military purposes, and on whether negotiations should focus solely on ICT infrastructure or on information content as well.

The second GGE was established after a five-year break for a session to be held in 2009/2010 under the Chair of Russia, with an identical task as the previous Group.²⁰ The 2010 consensus report recognized that cyber threats "are among the most serious challenges of the twenty-first century" and that they are capable of causing "substantial damage to economies and national and international security".²¹ The report detailed a variety of sources of threats, risks and vulnerabilities deriving for instance from the use of ICTs for malicious, criminal and terrorist purposes or as means of warfare, as well as from the attribution of cyber conducts, the protection of critical infrastructures and the use of proxies (paras. 4-11); it recommended cooperative measures (paras. 12-17); and it paved the way for future dialogue aimed at discussing norms, confidence-building and capacity-building measures, as well as stability and risk reduction measures and policies (para. 18).

¹⁸ James Lewis, 'Report of the International Security Cyber Issues Workshop Series' (2016) UNIDIR, Center for Strategic and International Studies, 22, available at: <www.csis.org/programs/strategic-technologies-program/archives/cybersecurity-and-governance/other-projects-5>.

¹⁹ Heli Tiirmaa-Klaar, 'The Evolution of the UN Group of Governmental Experts on Cyber Issues from a Marginal Group to a Major International Security Norm-Setting Body' (2021) *New Conditions and Constellations in Cyber*, Cyberstability Paper Series, 3-4.

²⁰ UNGA Res 60/45 (6 January 2006) UN Doc A/RES/60/45.

²¹ UNGA Res 65/201 (30 July 2010) UN Doc A/65/201 ('UNGGE 2010 Report'), para. 1.

The third UN GGE was established in 2011 with the mandate to “continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them, including norms, rules or principles of responsible behaviour of States and confidence-building measures with regard to information space” and to examine “relevant international concepts aimed at strengthening the security of global information and telecommunications systems”.²²

The 2013 report undisputedly recognized for the first time that international law norms and principles, including the UN Charter, apply to cyberspace and regulate States’ ICT-related conducts. The 2013 report listed recommendations of confidence and capacity-building measures (sections IV and V) respectively aiming at (i) increasing transparency, predictability and cooperation among States and (ii) improving ICT infrastructure security, developing technical skills and appropriate regulation, and bridging the divide in the security of ICTs and their use. More significantly, the GGE included a section (III) on norms, rules and principles of responsible behaviour of States containing recommendations on international obligations in cyberspace, ranging from States’ sovereignty on ICT-related activities and ICT infrastructures located on their territory, to the protection of human rights and fundamental freedoms, and State responsibility for wrongful acts.²³

The fourth GGE was established in 2014 with the mandate to continue the study on the norms, rules and principles of responsible State behaviour, on confidence and capacity-building measures, as well as on how international law applies to the use of ICTs by States, including in armed conflict.²⁴

The 2015 report expanded on the work of the previous report on norms, the application of international law, and confidence-building measures.²⁵ The GGE directed its discussions on the development of norms of a non-binding nature as separated from international law applicable in cyberspace. Namely, section III of the report lists 11 voluntary, non-binding norms, rules and principles for the responsible behaviour of States in their use of ICTs designed to prevent conflict in ICT environment and aimed at maintaining international peace, security and stability. These norms call for States’ cooperation in developing and applying measures to increase security and in preventing harmful ICT

²² UNGA Res 66/24 (13 December 2011) UN Doc A/RES/66/24, paras. 2-4.

²³ UNGA Res 68/98 (24 June 2013) UN Doc A/68/98 (‘UNGGE Report 2013’).

²⁴ UNGA Res 68/243 (9 January 2014) UN Doc A A/RES/68/243.

²⁵ UNGA Res 70/174 (22 July 2015) UN Doc A/70/174 (‘UNGGE 2015 Report’).

practices (13(a)), in the exchange of information and assistance in case of terrorist and criminal use of ICTs (13(d)) and in responding to requests for assistance by other States whose critical infrastructure is subject to malicious ICT acts (13(h)). Moreover, norms recommend that States should not knowingly allow their territory to be used for internationally wrongful acts by means of ICTs (13(c)); they should respect human rights obligations with specific reference to the right to privacy and freedom of expression (13(e)); they should not conduct or support ICT activity that damages critical infrastructure (13(f)) or the information systems of the authorized emergency response teams (13(k)); and they should enhance the protection of their critical infrastructure (13(g)).

With regards to section IV titled *How international law applies to the use of ICTs*, the 2015 report reiterates the full applicability of international law and the UN Charter to States' cyber activities and lists their international commitments that are deemed "of central importance", such as: "sovereign equality; the settlement of international disputes by peaceful means in such a manner that international peace and security and justice are not endangered; refraining in their 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 United Nations; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States".²⁶ Moreover, the report reaffirms States' jurisdiction over ICT infrastructure located in their territories; the applicability of the IHL principles of humanity, necessity, proportionality and distinction; the obligation not to use proxies to commit internationally wrongful acts; and the international obligations upon States deriving from internationally wrongful acts attributable to them under international law.²⁷

The fifth GGE convened at the end of 2015 with the task to continue the study of the previous GGEs (i.e. how international law applies to the use of ICTs by States; norms, rules, and principles of responsible behaviour of States; risks and threats in information security and possible measures to address them)²⁸ did not achieve a consensus report. The Governmental Experts reportedly did not agree on the application of specific norms

²⁶ UNGGE 2015 Report, para. 26.

²⁷ UNGGE 2015 Report, para. 28.

²⁸ UNGA res. 70/237 (30 December 2015) UN Doc A/RES/70/237.

relating to UN charter principles on the use of force and IHL, as well as countermeasures, by concern that it would lead to the militarisation of cyberspace.²⁹

Following the 2017 setback, the discussions regarding cybersecurity resumed at the UNGA in a tense geopolitical context. For the first time since the beginning of the negotiations, two resolutions on information security were adopted by the UNGA in the same year.³⁰ The first, Resolution 73/27 establishing an open-ended working group acting on a consensus basis was promoted by Russia and adopted on 5 December 2018.³¹ The second, resolution 73/266, promoted by the US, was adopted on 22 December 2018 and established a sixth and last GGE with the task to continue the study of the previous GGE iterations, namely possible cooperative measures to address existing and potential threats in the sphere of information security, including the norms of responsible behaviour, capacity-building and confidence-building measures, and international law. With respect to the latter, the UNGA additionally requested that States participating in the GGE submit national contributions about how international law applies to the use of ICTs by States to be included in an annex to the final report.³² The sixth GGE's mandate additionally includes consultations to be held with the main regional organizations, such as the AU, the EU, the OAS, the OSCE, the ASEAN Regional Forum (ARF).³³

The 2021 GGE report on *Advancing responsible State behaviour in cyberspace in the context of international security* continued with the discussion on the existing and emerging threats in the ICT environment, as well as the confidence-building and capacity-building measures addressed to States. The report expands on the 11 norms, rules and principles enunciated in the 2015 report by further detailing them and discusses international law applicable to cyberspace and ICT-related activities by States.³⁴

²⁹ Arun M. Sukumar, 'The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?', in Lawfare, available at <www.lawfaremedia.org/article/un-gge-failed-international-law-cyberspace-doomed-well>; Cuba, 71 UNGA: Cuba at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Representaciones Diplomáticas de Cuba en El Exterior, 23 June 2017; Russia, Response of the Special Representative of the President of the Russian Federation for International Cooperation on Information Security Andrey Krutskikh to TASS' Question Concerning the State of International Dialogue in this Sphere, Ministry of Foreign Affairs of the Russian Federation, 29 June 2017.

³⁰ François Delerue, Frédéric Douzet, Aude Géry, 'The Geopolitical Representations of International Law in the International Negotiations on the Security and Stability of Cyberspace' (2020) Report No. 75, IRSEM/EU Cyber Direct, 19.

³¹ See below, section 1.2.

³² UNGA Res 73/266 (22 December 2018) UN Doc A/RES/73/266.

³³ UNODA, *Developments in the field of information and telecommunications in the context of international security*, Fact Sheet, available at <<http://www.un.org/disarmament/ict-security>>.

³⁴ UNGA Res 76/135 (14 July 2021) UN Doc A/76/135 ('UNGGE 2021 Report').

Section IV of the report, titled *International law*, reaffirms the conclusions of the previous GGEs, namely that international law, and in particular the UN Charter is applicable to ICT-related conducts by States environment and is essential to maintaining peace and stability and for promoting an open, secure, stable, accessible and peaceful ICT environment.³⁵ In addition to the commitments of States to the principles detailed in the 2015 report, the sixth GGE further details that: in accordance with the international obligations under Article 2(3) and Chapter VI of the UN Charter, States should solve their disputes involving cyber means peacefully;³⁶ State sovereignty and deriving international norms and principles apply to the States' cyber activities and to their jurisdiction over ICT infrastructure within their territory;³⁷ States must respect the principle of non-intervention in the internal affairs of another State, including by means of ICTs;³⁸ States should refrain from the threat or use of force against the territorial integrity or political independence of any State in their international relations;³⁹ IHL and its principles of humanity, necessity, proportionality and distinction apply in armed conflict (although further study is required);⁴⁰ States must meet their international obligations regarding internationally wrongful acts that are attributable to them under international law.⁴¹ With regards to this last aspect, the GGE reaffirmed that States must not use proxies to commit internationally wrongful acts using ICTs and should not allow their territories being used to commit the aforementioned acts. At the same time, the GGE – while acknowledging that “invocation of the responsibility of a State for an internationally wrongful act involves complex technical, legal and political considerations” – noted that the fact that an ICT activity is “launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State” and that “accusations of organizing and implementing wrongful acts brought against States should be substantiated”.⁴²

³⁵ UNGGE 2021 Report, para. 70-71.

³⁶ UNGGE 2021 Report, para. 71(a).

³⁷ UNGGE 2021 Report, para. 71(b).

³⁸ UNGGE 2021 Report, para. 71(c).

³⁹ UNGGE 2021 Report, para. 71(d).

⁴⁰ UNGGE 2021 Report, para. 71(f).

⁴¹ UNGGE 2021 Report, para. 71(g).

⁴² Ibid.

1.2 The UN Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG)

In 2018, with Resolution 73/27, the UNGA convened an Open-Ended Working Group (OEWG) with the mandate to (i) continue to further develop the rules, norms and principles of responsible behaviour of States, and the ways for their implementation; (ii) continue the study on existing and potential threats in the sphere of information security and possible cooperative measures to address them (i.e., confidence-building and capacity-building measures); (iii) further address the issue of how international law applies to the use of ICTs by States; (iv) establish regular institutional open-ended dialogue within the UN; and (v) examine relevant international concepts for strengthening the security of global IT systems.⁴³ The OEWG, which published a consensus report in 2021, was renewed for a second iteration for 2021/2025.⁴⁴

Differently to the GGE, whose participation is limited to a number of selected States, and which carries on consultations with the main regional organizations, the OEWG is open to all UN Member States and holds intersessional consultative meetings with business, non-governmental organizations and academia.

1.2.1 The OEWG 2019/2020

The first OEWG iteration began its works on 3-4 June 2019, and gathered representatives of almost 100 States. It held three substantive sessions between 2019 and 2021 and an intersessional consultative meeting in 2019.

The 2021 OEWG report reaffirmed the conclusions of the previous GGEs, namely with respect to the norms for responsible State behaviour and the assertion that international law, including the UN Charter, is applicable to cyberspace. However, the OEWG does not further deepen the discussion on how international law applies to cyber activities, but merely reaffirms the general applicability of its norms and principles, including the general obligation on States to solve their disputes by peaceful means, including those by ICT means (paras. 34-40).⁴⁵

⁴³ UNGA Res 73/27 (5 December 2018) UN Doc A/RES/73/27.

⁴⁴ UNGA Res 75/240 (4 January 2021) UN Doc A/Res/75/240.

⁴⁵ UNGA Conference Room Paper (10 March 2021) UN Doc A/AC.290/2021/CRP.2 ('OEWG 2021 Report').

Alongside the assessment of existing and potential threats (paras. 15-23) and of capacity and confidence-building measures to address them (paras. 41-67), the OEWG 2021 Report acknowledges the importance of “voluntary, non-binding norms of responsible behaviour” (paras. 24-33) in reducing the risks associated with the misuse of ICTs and the prevention of conflicts in ICT environment. The Report recalls that these norms “do not replace or alter States’ obligations or rights under international law” but “rather provide additional specific guidance on what constitutes responsible State behaviour in the use of ICTs”. Moreover, it acknowledges that additional norms could be developed over time.

Paragraph 80 of the OEWG 2021 Report (*Final Observations*) acknowledges that the negotiations within the Group welcomed “diverse perspectives” that “were not necessarily agreed by all States, including the possibility of additional legally binding obligations” regarding ICT environment regulation.

1.2.2 The OEWG 2021/2025

On 4 January 2021, the OEWG was renewed for a second iteration to be held in 2021/2025 with a very similar mandate of the first Group and “with a view to ensuring the uninterrupted and continuous nature of the democratic, inclusive and transparent negotiation process on security in the use of information and communications technologies, under the auspices of the United Nations”.⁴⁶

The composition of the second OEWG is also open, allowing all those UN Member States that express interest to participate. Upon request of the UNGA, the delegations at the OEWG have reached compromise on two annual progress reports to date, in July 2022⁴⁷ and July 2023.⁴⁸

As it has been observed in legal doctrine and by commentators, however, while States have reached some progress in confidence-building measures and capacity building, they have not gone much further on the study of international law but, limited themselves to reaffirming the principles contained in the previous reports.⁴⁹

⁴⁶ UNGA Res 75/240 (4 January 2021) UN Doc A/Res/75/240.

⁴⁷ UNGA Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025 (8 August 2022) UN Doc A/77/275.

⁴⁸ UNGA Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025 (1 August 2023) UN Doc A/78/265.

⁴⁹ With reference to the first Annual report, see for instance, Pietro Gargiulo, ‘Nazioni Unite, Cybersecurity e Diritto Internazionale’ in Ornella Porchia and Michele Vellano (eds), *Il Diritto Internazionale per la Pace e nella*

1.3 Future processes: The Programme of Action (PoA) for Advancing Responsible State Behaviour in Cyberspace

Against the background of the negotiation processes discussed above, France and over 40 other States (including the EU and its member States) proposed a Programme of Action for advancing responsible State behaviour in cyberspace with a view to ending the dual track discussions and establishing a permanent UN forum to consider the use of ICTs by States in the context of international security.⁵⁰

The proposal acknowledges that the dual track negotiations might be counterproductive and hence suggests the establishment of a permanent, inclusive, action-oriented mechanism, whose modalities could be discussed within the ongoing OEWG.

In 2022, the UNGA First Committee adopted Resolution 77/37⁵¹ welcoming the proposal to establish a *Programme of Action to advance responsible State behaviour in the use of information and communications technologies in the context of international security* (Cyber PoA) at the end of the current OEWG (2025).

The Cyber PoA will be set up with a view to (i) discuss existing and potential threats; (ii) to support States' capacities and efforts to implement and advance commitments regarding the framework for responsible State behaviour, including the voluntary, non-binding norms for the application of international law to the use of ICTs by States, confidence-building and capacity building measures.⁵²

With a view to discuss the modalities for the establishment of the PoA, Resolution 77/37 also requires that the UNSG seek voluntary contributions by Member States on the scope, structure, and content of the PoA, and that the UN Office for Disarmament Affairs of the Secretariat (UNODA) collaborate with relevant regional organizations to convene consultations to share views on the PoA.

Guerra, Sviluppi Recenti e Prospettive Future, Liber Amicorum in Onore di Edoardo Greppi (Edizioni Scientifiche Italiane 2023) 67.

⁵⁰ "The future discussions on ICTs and cyberspace at the UN" (10 August 2020), available at <<https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf>>.

⁵¹ The resolution was adopted by a recorded vote of 157 in favour, and 6 against. Fourteen States abstained.

⁵² UNGA res. 77/37 (12 December 2022) UN Doc A/RES/77/37.

2. The Role for the EU and EU Member States within UN Processes devoted to Cyber Issues

Since the beginning of the negotiations within the UN, the EU and EU Member States have played a role in the diplomatic initiatives discussed above.

A number of EU Member States have regularly taken part in the various GGE iterations, notably in the 2004/2005 GGE (France, Germany, UK); the 2009/2010 GGE (Estonia, France, Italy, UK); the 2012/2013 GGE (Estonia, France, Germany, UK); the 2014/2015 GGE (Estonia, France, Germany, Spain, UK); the 2016/2017 GGE (Estonia, Finland, France, Germany, Netherlands); and the 2019/2021 GGE (Estonia, France, Germany, Netherlands, Romania).

Following the UNGA invitation in resolution 73/266 to submit national contributions on the application of international law to ICTs, fifteen of the twenty-five participating governmental experts submitted their views, which were later included in an Official compendium of voluntary national contributions annexed to the GGE 2021 final report.⁵³ Among them, Estonia, Germany, the Netherlands, and Romania submitted their views.

In addition to GGE participating States, other EU Member States have made their positions on the applicability of international law to ICT environment and ICT-related conducts by States public.⁵⁴ The national positions of EU Member States that have been made public so far both autonomously and within the GGE process, twelve in total, have generally shown a high level of convergence among them.⁵⁵

Within the established framework of collaboration between the sixth GGE on *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* and regional organizations pursuant to resolution 73/266, the consultations organized by

⁵³ UNGA Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266 (13 July 2021) UN Doc A/76/136

⁵⁴ Czech Republic, Denmark, Finland, France, Ireland, Italy, Poland, Sweden. Source: International Cyber Law in Practice: Interactive Toolkit, at <https://cyberlaw.ccdcoe.org/wiki/List_of_articles#National_positions>, accessed November 2023.

⁵⁵ François Delerue, 'Towards an EU Position on the Application of International Law in Cyberspace' (8 June 2023) EU Cyber Direct, Briefing Paper, available at <<https://eucyberdirect.eu/research/toward-an-eu-position-on-the-application-of-international-law-in-cyberspace>>.

UNODA with the EU were carried out from 19-20 June 2019 in Brussels, within the context of the EU Horizontal Working Party on Cyber Issues (HWP).⁵⁶

The consultations raised several issues, ranging from the risks posed by “lower-level ICT-threats”, including the potential impact on peace and security of interference in democratic processes by cyber means; to the need “for greater awareness-raising and capacity-building of States” and “a human-centric approach to cybersecurity”, which has regard for rights in ensuring a stable and peaceful cyberspace. With respect to the framework of responsible State behaviour, the consultations highlighted a general adherence of the EU to the cyber norms developed by the GGEs, while at the same time emphasised the need of discussing their implementation, rather than modifications, and the possibility than additional norms are introduced. On international law, the possibility that the EU develops a “overarching statement” on the issue has been raised by some.⁵⁷

Lastly, the moderating role of the EU in intergovernmental processes was emphasised. The consultations highlighted that the EU “should act as a force for good in the world and in the promotion of a rules-based and human rights-based cyberspace” and that it “could also play a lead role in discussions related to the protection of privacy of data and undue intervention on democratic institutions”.⁵⁸

The EU and its Member States have also participated in the OEWG process, in both the first and second iteration currently underway.⁵⁹ In the joint comments⁶⁰ to the draft report of the OEWG, the EU and its Member States have shown adherence to the agreements reached by the GGE reports, while at the same time welcoming the transparency and inclusiveness of the OEWG. Considering the potentially devastating humanitarian consequences of attacks on critical infrastructure (CI) and critical information

⁵⁶ Collated summaries of the Regional Consultations series of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, First substantive session of the Group of Governmental Experts (9-13 December 2019), available at: <<https://disarmament.unoda.org/group-of-governmental-experts/>>.

⁵⁷ Ibid., pp. 11-13.

⁵⁸ Ibid.

⁵⁹ See, e.g. UNGA Compendium of statements in explanation of position on the final report, Third substantive session (25 March 2021) UN Doc A/AC.290/2021/INF/2.

⁶⁰ Joint comments from the EU and its Member States on the initial ‘pre-draft’ report of the Open-Ended Working Group on developments in the field of Information and Telecommunication in the context of international security, available at: <<https://front.un-arm.org/wp-content/uploads/2020/05/eu-contribution-alignments-oewg.pdf>>, 3ff. For a report on the discussion within OEWG’s substantive sessions, see e.g. ‘UN OEWG – Our reports and blogs’, available at: <<https://dig.watch/processes/un-gge>>.

infrastructure (CII), they endorsed the applicability of the norms of responsible behaviour and international law to ICT-related conducts by States (paras. 18-21).

With respect to international law, the EU and its Member States claimed the centrality of existing international law, including the UN Charter, international human rights law (IHRL) and IHL for a universal cyber security framework (para 21) and opposed the views that question the agreed consensus on international law reached by the previous GGEs (para. 27). Significantly, in their view, the applicability of IHL shall not be seen as legitimising the use of force between States in ICT environment (para. 22).

With respect to the rules, norms and principles for responsible State behaviour, the EU and its Member States once again welcomed the consensus reached by the 2015 GGE report, endorsing the repeated calls on States to be guided by them in their use of ICTs and further implementation of the agreed norms and confidence-building measures, also in light of their fundamental role in maintaining peace and preventing conflict in cyberspace (para. 28).

Conversely, the position of the EU and its Member States reveals an objection towards the possibility of developing a new legal cyber-specific instrument. This is also due to the concern that the divisive and lengthy process would carry the risks of “undermining the ongoing practical efforts to tackle the real, pertinent and pressing problem of increasing cyber incidents, and also risks impacting on work aimed at preventing conflict prevention and promoting stability in cyberspace”.⁶¹ In this regard, efforts should be aimed at the implementation and better understanding of the eleven norms of responsible State behaviour and building “capacities for States in the areas of international law, national legislation and policy in order to enhance a common understanding as to how existing international law applies to the use of ICTs by States.”⁶²

In the 2020 EU’s Cybersecurity Strategy for the Digital Decade⁶³ presented by the European Commission and the High Representative for Foreign Affairs and Security Policy, the importance of international cooperation in maintaining a global, open, stable and

⁶¹ Joint comments from the EU and its Member States on the initial ‘pre-draft’ report of the Open-Ended Working Group on developments in the field of Information and Telecommunication in the context of international security, available at: <<https://front.un-arm.org/wp-content/uploads/2020/05/eu-contribution-alignments-oewg.pdf>>, 14ff.

⁶² Ibid.

⁶³ European Union, European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament and the Council, The EU’s Cybersecurity Strategy for the Digital Decade, JOIN(2020)18 final, 16 December 2020.

secure cyberspace was addressed. In this light, “the EU continues to work with international partners to advance and promote a global, open, stable and secure cyberspace where international law, in particular the United Nations (UN) Charter, is respected, and the voluntary non-binding norms, rules and principles of responsible state behaviour are adhered to”.⁶⁴

In regards to the purpose of advancing responsible State behaviour in cyberspace and in light of the “deterioration of an effective multilateral debate on international security in cyberspace” the need for the EU to take a proactive posture within the discussion regarding cybersecurity at the UN and other fora was highlighted, with a view to (i) advancing, coordinating and consolidating Member States’ positions in international fora; and (ii) developing an EU position on the application of international law in cyberspace.⁶⁵

Similar positions were recently supported by the Council of the European Union in its conclusions on the development of the European Union's cyber posture approved on 23 May 2022, in which it reiterated the EU’s need to develop its cyber posture, as well as its approach towards a cybersecurity aimed at contributing to conflict prevention and enhancing stability in international relations. The Council hence reaffirms the applicability of international law (including IHL and IHRL) to States cyber activities, as well as EU’s commitments to act in accordance with the voluntary, non-binding norms of responsible State behaviour in cyberspace agreed by the GGEs. At the same time, the conclusions reaffirm EU’s commitment to promoting its values and principles based on human rights, fundamental freedoms, and the rule of law.⁶⁶

Notwithstanding the declared need and will to adopt a common position on the matter, it has been discussed that EU Member States appeared to have been working independently within the UN mechanisms undertaken so far and have seemed incapable, for the moment, to offer a unified voice within cyber negotiations.⁶⁷ However, the EU may play a conciliative role among diverging positions regarding cybersecurity, especially in light of its expertise on the implementation of its international obligations on the

⁶⁴ Ibid., p. 20.

⁶⁵ Ibid.

⁶⁶ EU Council, Council conclusions on the development of the European Union's cyber posture (23 May 2022) No. 7925/18.

⁶⁷ Delerue *et al.* (n 30) 22ff.

matter,⁶⁸ with a view to protecting its interests and promoting the essential of human rights in ensuring a stable and peaceful cyberspace.⁶⁹

Finally, as anticipated above, the EU has been among the 40 States, together with France, to propose and sponsor the establishment of a Cyber PoA, with a view to strengthening the implementation of the framework for responsible State behaviour.⁷⁰

3. The Framework of Responsible State Behaviour in Cyberspace

The landmark consensus achieved by States in the UN negotiations regarding cybersecurity has represented a significant advancement in the discussion regarding the international legal framework applicable to ICT environment and ICT-related conducts. In their reports, the GGEs and the OEWG have unambiguously affirmed that international law applies to cyberspace and that States cyber activities do not occur in a legal vacuum but are regulated by international law norms and principles.

Moreover, the list of 11 norms, rules and principles of responsible State behaviour enshrined in the 2015 GGE report was subsequently welcomed and endorsed by the UNGA resolution 70/237⁷¹, which recommended States to be guided by them in their cyber activities, and were incorporated in subsequent resolution 73/27.⁷² Moreover, they were reaffirmed by the GGE and OEWG reports published in 2021. Additionally, the norms found endorsement by States⁷³ and by a variety of regional organizations, e.g. the EU and Association of Southeast Asian Nations (ASEAN)⁷⁴.

⁶⁸ Ibid. (reference is made to the NIS directive and GDPR).

⁶⁹ On the EU position on the application of international law in cyberspace, see e.g., François Delerue, Aude Géry, 'International Law and Cybersecurity Governance: The Way Forward' in François Delerue and Aude Géry (eds) *International Law and Cybersecurity Governance* (EU Cyber Direct, July 2022); François Delerue, 'Towards an EU Position on the Application of International Law in Cyberspace' (8 June 2023) EU Cyber Direct, Briefing Paper, available at <<https://eucyberdirect.eu/research/toward-an-eu-position-on-the-application-of-international-law-in-cyberspace>>.

⁷⁰ See, e.g. Council conclusions (n 66), paras. 20-21; see also section 1.3.

⁷¹ UNGA Res 70/237 (30 December 2015) UN Doc A/RES/70/237.

⁷² UNGA Res 73/27 (n 43).

⁷³ See, e.g. positions of GGE States in the UNGA Official compendium of voluntary national contributions (n 53).

⁷⁴ EU Council, Council Conclusions on malicious cyber activities (16 April 2018) No. 7925/18; ASEAN Leaders' Statement on Cybersecurity Cooperation (2018) 32nd ASEAN Summit, available at <<https://asean.org/wp-content/uploads/2018/04/ASEAN-Leaders-Statement-on-Cybersecurity-Cooperation.pdf>>.

3.1 Norms, rules and principles for the responsible behaviour of States

When it comes to the Framework of Responsible State Behaviour (or the *acquis*) in cyber negotiations, reference is usually made to the body of existing agreements (GGE 2013 report; GGE 2015 report; GGE 2021 report; and OEWG 2021 report), although with a certain degree of unclarity on the matter.⁷⁵

In terms of content of the *acquis* and the scope of the voluntary, non-binding norms, these are framed as representations of the international community's expectations in the cyber domain, and they set standard behaviour that States should adopt when performing their activities by means of ICTs.⁷⁶

In general terms, these norms call for States' cooperation in the development and application of measures that are aimed at increasing stability and security in their use of ICTs, as well at preventing harmful ICT practices, with the purpose of maintaining peace and security.⁷⁷

States should as well cooperate in the exchange of information and assistance in the prosecution of terrorist and criminal use of ICTs, in the implementation of cooperative measures to counter related threats,⁷⁸ and in responding to requests for assistance by other States whose critical infrastructure is subject to malicious ICT acts.⁷⁹

When it comes to the enhancing of security measures, States should take reasonable steps to protect the supply chain and prevent the proliferation of malicious ICT tools and techniques,⁸⁰ and should take appropriate measures to protect their critical infrastructure from ICT threats pursuant to UNGA Resolution 58/199⁸¹ on the Creation of a global culture of cybersecurity and the protection of critical information infrastructures (and its annex).⁸²

⁷⁵ One example refers to resolutions 73/27 and 73/266 respectively establishing the OEWG and the sixth GGE, which have defined the mandate of the Groups. The norms contained in the two resolutions slightly differ. See, on the matter, Delerue et al. (n 67) 26ff.

⁷⁶ UN GGE 2021 Report, para. 15.

⁷⁷ UN GGE 2021 Report, Norm 13 (a).

⁷⁸ UN GGE 2021 Report, Norm 13 (d).

⁷⁹ UN GGE 2021 Report, Norm 13 (h).

⁸⁰ UN GGE 2021 Report, Norm 13 (i).

⁸¹ UNGA Res. 58/199 (23 December 2003) UN Doc. A/RES/58/199.

⁸² UN GGE 2021 Report, Norm 13 (g).

With specific regards to ICT vulnerabilities, States should encourage their responsible reporting, and should as well share pertinent information on remedies aimed at listing and possibly eliminating threats to ICTs and ICT-dependent infrastructure.⁸³

Moreover, norms recommend that – in case of ICT-related incidents – States should consider relevant information, including the context, the challenges of attribution in the ICT environment,⁸⁴ the nature and the extent of the consequences,⁸⁵ to prevent the inter-State escalation of tensions.⁸⁶

States are recommended not to knowingly allow their territories to be used for internationally wrongful acts by ICT means and to hence take all appropriate and reasonable measures available, in the event that they become aware or are notified that an internationally wrongful act conducted using ICTs is emanating from or transiting through their territories.⁸⁷

Moreover, they should not conduct or knowingly support ICT activity that is contrary to their international obligations and that is intentionally directed at damaging or impairing the use or operation of critical infrastructure that provides essential services to the public (e.g., health care and medical infrastructure and facilities, energy, power generation, water and sanitation, education, commercial and financial services, transportation, telecommunications and electoral processes, as well as the general availability or integrity of the Internet).⁸⁸

Finally, with the purposes of ensuring a secure ICT employment, States should respect and protect human rights obligations and fundamental freedoms both online and offline, by taking specific consideration of Human Rights Council Resolutions on the promotion,

⁸³ UN GGE 2021 Report, Norm 13(j).

⁸⁴ Attribution refers to the process through which a conduct can be imputed to the perpetrator. One fundamental aspect concerns the legal attribution of a conduct (especially when unlawful under international law) to State. In the cyber realm, the attribution of a cyber conduct is particularly hard, since it requires technical, political, and legal considerations. The three main dimensions that come into play when determining to whom a certain operation may be imputed are: the attribution of the cyber operation to the machine; the attribution to the individual(s) who conducted said operation; and the attribution of the cyber operation to the State. See, e.g., François Delerue, *Cyber Operations and International Law* (CUP 2020), 51ff; Marco Roscini, 'Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations' in Jens David Ohlin, Kevin Govern, Claire Finkelstein (eds) *Cyber War: Law and Ethics for Virtual Conflicts* (OUP 2015).

⁸⁵ The aspects to consider in the assessment of the incidence should be substantiated by facts and can include the incident's technical attributes; its scope, scale and impact; the wider context, including the incident's bearing on international peace and security; and the results of consultations between the States concerned.

⁸⁶ UN GGE 2021 Report, Norm 13 (b).

⁸⁷ UN GGE 2021 Report, Norm 13 (c).

⁸⁸ UN GGE 2021 Report, Norm 13 (f).

protection and enjoyment of human rights on the internet (HRC resolutions 20/8 and 26/3); General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age; and the right to freedom of expression.⁸⁹ Specific reference is made to the obligations of States deriving from international law, i.e. relevant provisions of the International Covenant on Civil and Political Rights, the International Covenant on Economic, Social and Cultural Rights and the Universal Declaration of Human Rights, especially dealing with the “freedom to seek, receive and impart information regardless of frontiers and through any media” and whose observance “can also contribute to promoting non-discrimination and narrowing the digital divide, including with regard to gender”.⁹⁰

3.2 Main Open Issues

The legal nature of the cyber norms, as well as their relationship with international obligations of States has been the object of debate in legal doctrine. As noted, although widely endorsed, the UNGA resolutions are not binding on States. Moreover, the GGE and OEWG reports framed the norms of responsible State behaviour as “voluntary” and “non-binding”. As a matter of fact, the norms are not meant to replace nor alter States’ international obligations or rights deriving from international law (which are binding), nor they seek to limit or prohibit behaviour that would be otherwise consistent with international law. Conversely, they are rather designed to provide guidance for States with respects to what constitutes their responsible behaviour in cyberspace.⁹¹

However, as the list of norms developed by the UN GGE process include different sets of provisions aimed at setting standards for the responsible behaviour of States in cyberspace, the relationship between cyber norms and existing legal and policy instrument has generated discussions. Although there exist various views on the matter, according to the prevalent view among international law scholars, not all norms comply with the voluntary and non-binding nature but derive or reflect existing international law.⁹²

⁸⁹ UN GGE 2021 Report, Norm 13 (e).

⁹⁰ Ibid., paras. 36 ff.

⁹¹ UN GGE 2021 Report, para. 15; UN OEWG 2021 Report, para. 25.

⁹² Eneken Tikk (ed) *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology, A Commentary*, Civil and Society Disarmament, United Nations Office for Disarmament Affairs (UNODA, 2017), 4-5.

Some of these norms, including for instance the domestic measures and good practices that States should adopt to in order to enhance and strengthen the stability of ICT environment (e.g., relating to the reporting of vulnerabilities, to the integrity of the supply chain, and to the protection of the critical infrastructure) appear to comply with the voluntary and non-binding nature of the cyber norms.⁹³

On the contrary, other norms are either grounded on or derive from international law existing obligations. These relate for instance to the general recommendation for inter-State cooperation with the purposes of increasing stability in ICT environment and maintaining peace and security, which may be inferred from international existing obligations specifically relating to the duty of cooperation under the UN Charter.⁹⁴ Similarly, the recommendation to ensuring assistance in the event of malicious (either criminal or terrorist) use of ICTs may be derived from existing conventional obligations relating to counter terrorism and criminal law.⁹⁵

The norm according to which States should not knowingly allow their territory to be used to commit internationally wrongful acts may refer to the legal concept of due diligence despite with some specificities.⁹⁶

Another example relates to the norm calling for States' respect and protection of human rights and fundamental freedoms in cyberspace, which makes explicit reference to relevant international treaties and HRC resolutions without further interpretations and has been described as a "mere reminder of existing obligations".⁹⁷

The (often artificial) distinction between on the one side norms of responsible State behaviour, and on the other side international obligations "disregards the link that exist between certain non-binding provisions and some binding obligations".⁹⁸ In general terms, the GGEs' orientation towards the adoption of non-binding norms and principles as somehow distinct to international law section, together with the opaqueness concerning their relationship with existing legal and policy instruments, has introduced a

⁹³ Marja Lehto, 'The rise of cyber norms' in Nicholas Tsagourias and Russell Buchan (eds) *Research Handbook on International Law and Cyberspace* (Edward Elgar 2021), 39ff.

⁹⁴ Ibid., 39, citing: UN Charter arts 1(1), 3; UNGA Res 2625 (24 October 1970) UN Doc A/RES/2625(XXV).

⁹⁵ Ibid.

⁹⁶ Liisi Adamson, 'Recommendation 13 (c)' in Tikk (n 92).

⁹⁷ Lehto (n 93), 40. With reference to the UN GGE 2015, see also Barrie Sander, 'Recommendation 13 (e)', in Tikk (n 92).

⁹⁸ Delerue *et al.* (n 30), 31.

certain degree of confusion in the discourse on regulation of cyberspace and the applicable framework to ICT-related conducts.⁹⁹

In this framework, said distinction – together with the incapability or unwillingness of States within these processes to agree on “hard” law or to clarify the scope of the cyber norms – may be partially derived from (i) different views on the regulation of digital technologies, and (ii) the intrinsic political nature of normative development regarding cybersecurity.

First, cyber negotiations have been characterized since their early days by divergence of approaches. During the various GGE and OEWG iterations, some States (including for instance China, Russia, and Cuba) have supported the idea that existing international law does not offer a proper framework to regulate the use of ICTs and ICT environment, and have advocated for the development of *lex specialis*, including possibly multi-lateral binding cyber-specific regulation. On the contrary, the approach of the Western States (with United States on the lead) has highlighted the suitability of existing international legal framework, without however effectively providing a clear understanding of how norms should be interpreted in the specific context of ICTs.¹⁰⁰

Second, the debate over ICT environment regulation is incardinated in geopolitical dynamics and ideological and strategical differences surrounding cybersecurity. Some of the difficulties in reaching agreement on ICTs regulation is not much legal as it is political. States have indeed employed the platforms offered by cyber negotiations to impose their ideological representations of cyberspace, by advancing different and competing priorities such as economic prosperity, human rights or fundamental freedoms on the one hand, or information security on the other.¹⁰¹

Without disregarding the legal obligations of States in cyberspace, the choice towards the adoption of non-binding cyber norms has been described in this context as a “palliative to international law”. In this sense, these norms allow States to agree on the interpretation of specific international obligations without “setting them in stone” and may

⁹⁹ See, *inter alia*, Eneken Tikk ‘Introduction’ in Tikk (n 92), 3–4; Liisi Adamson, ‘International Law and International Cyber Norms’ in Dennis Broeders and Bibi van den Berg (eds), *Governing Cyberspace: Behavior, Power and Diplomacy* (Rowman & Littlefield International 2020); Lehto (n 93); Delerue *et al.* (n 30), 29.

¹⁰⁰ Adamson (n 99), 26; Anders Henriksen, ‘The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace’ (2019) *Journal of Cybersecurity* 5, 4–5.

¹⁰¹ *Ibid.*, 5ff.

serve as a basis to further discuss the applicable framework or the formation of new obligations (e.g. through a new treaty or customary rules).¹⁰²

Despite the longstanding negotiations regarding cybersecurity and ICT regulations, various issues specifically concerning the application of international law to digital technologies and States' cyber activities remain open. These do not concern solely the debate over the possible development of additional cyber-specific norms but relate to the question on *how* pertinent norms and principles stemming from *jus in bello*, *jus ad bellum*, State responsibility, or international human rights apply to States' ICT-related conducts.

The most relevant points of contention that are still the object of discussion indeed include e.g. the problem of attributing cyber conducts to States, the use of force by means of cyber operations and the threshold required under Article 2(4) of the UN Charter, the principle of non-intervention in the internal or external affairs of other States, the due diligence concept and its legal quality, countermeasures by third States, and certain rules of IHL applicable to international and non-international armed conflicts.¹⁰³

¹⁰² Delerue *et al.* (n30), 57ff.

¹⁰³ See, in general, Henning Lahmann, 'State Behaviour in Cyberspace: Normative Development and Points of Contention' (2023) *Zeitschrift für Außen- und Sicherheitspolitik* (ZfAS) 16:31–41.

Part B – Data processing for international policies: empirical perspective (UNIBO)

1 The issue of Data Quality for policy decisions.

1.1 Introduction

The overall goal of this part of SERICS-EcoCyber is to explore the various policy solutions that have been adopted, researched, and discussed to respond to the increased need for security in cyberspace. Policies, however, are as good as the information and data on which policy decisions are made. One consistent problem, which we have selected as our main research topic, is the quality of data (type, consistency, and above all, relevance) that is being used to develop policy solutions. It is hardly surprising that (according to one survey by one of the most reputable coding developers), data scientists spend the largest portion of their time preparing and cleaning the data.¹⁰⁴ On top of such obstacles, cybersecurity is even more problematic and challenging: the malicious actors that target infrastructures and computer networks have as guiding principle to avoid detection and identification, thus adopting all possible means to “hide” or, at least, make deniability “plausible”, particularly if they are somehow attached to or sponsored by sovereign governments. This state of affairs have made the *problem of attribution* (i.e. identifying the culprits so that they could be prosecuted in the court of law) one of the major obstacle for security in cyberspace.¹⁰⁵

The relevant literature on why quality and availability of data matter overwhelmingly when it comes to cyberspace (and therefore cybersecurity) is rather extensive and spans a few decades (and it started with cybercrime and cyberwarfare). In the footnote,¹⁰⁶ we

¹⁰⁴ Anaconda is one of the most important developers of Python suites; see Anaconda (2022) “The State of Data Science”, available at <https://www.anaconda.com/resources/whitepapers/state-of-data-science-report-2022> (accessed 21 November 2023).

¹⁰⁵ Florian J. Egloff & Max Smeets (2021) “Publicly Attributing cyber attacks: A Framework,” *Journal of Strategic Studies*, DOI: 10.1080/01402390.2021.1895117.

¹⁰⁶ One of the earliest examples is Giacomello, G. (2003), «Measuring ‘Digital Wars’: Learning From the Experience of Peace Research and Arms Control», *The Information Warfare Site Infocon Magazine* 1, October; also, see, for example, L. Jean Camp, Lorrie Cranor, Nick Feamster et al. (2009) “Data for Cybersecurity Research: Process and Wish List”, January, available at https://www.researchgate.net/publication/255960171_Data_for_Cybersecurity_Research_Process_and_Wish_List, Florêncio, D. & Herley, C. (2013) “Sex, lies and cyber-crime surveys”. in *Economics of information security and privacy III* (pp. 35-53). Springer, New York, NY; George Grispos, William Glisson, Tim Storer

just limited ourselves to a few references, as an extensive literature review is outside the scope of this report. Furthermore, and more importantly, articles and papers mostly point out and bring to the fore the themes we illustrated in the opening paragraph of this report, namely that (a) data on cybersecurity is hard to collect (b) it is often incompletable, (c) it suffers from problems of (1) reliability and (2) validity¹⁰⁷ and (d) malicious actors, both state and non-state actors, go to extreme lengths to hide their identities, actions and geographical and political origins. Indeed, it has been noted that:¹⁰⁸

Industry and academia have also been unable to fill the gap. Academic researchers generally study cyber incidents reported in the press, but much of cyber conflict remains covert or is never publicly reported. Companies providing cyber security services have a wealth of incident data, and insurance companies gather details from cyber-related claims. However, this data is proprietary, which has limited its use and access.

As we have seen, it is a well-established fact that today, cybersecurity is one of the 'hottest' topics when approaching cyberspace: it is on the media, in academia and there is a persistent complaint that there are not enough cybersecurity specialists. Measuring in cyberspace has long been a challenge, since the early days of 'the Net'.¹⁰⁹ While such situation has considerably improved and there are increasing 'measures' of different features of cyberspace, researching security in cyberspace is still a rather challenging undertaking. Security comes from the Latin *se curare*, namely, taking care of someone

(2019) "How Good is Your Data? Investigating the Quality of Data Generated During Security Incident Response Investigations", Preprint, January, available on https://www.researchgate.net/publication/330382307_How_Good_is_Your_Data_Investigating_the_Quality_of_Data_Generated_During_Security_Incident_Response_Investigations; Roberto Omar Andrade, Nicole Ontaneda, Andrea Silva et al. (2020) "Application of Big Data Analytic in Cybersecurity", paper Conference at Application of Big Data Analytic in Cybersecurity, January Cognitive security Lab, available at https://www.researchgate.net/publication/338582915_Application_of_Big_Data_Analytic_in_Cybersecurity; Yerina, A. M., Honchar, I. A., and Zaiets, S. V. (2021) "Statistical Indicators of Cybersecurity Development in the Context of Digital Transformation of Economy and Society". *Science and Innovation*, V. 17, no. 3. pp. 3—13., <https://doi.org/10.15407/scine17.03.003>; Valeriano, B. (2022) "The need for cybersecurity data and metrics: empirically assessing cyberthreat", *Journal of Cyber Policy*, DOI: 10.1080/23738871.2022.2111997;

¹⁰⁷ See for example, Trochim, W.M. *The Research Methods Knowledge Base*, 2nd ed. Available at <http://www.socialresearchmethods.net/kb/> (accessed 30 November 2023) and Carmines, E.G. & Zeller, R.A. (1979) *Quantitative Applications in the Social Sciences: Reliability and Validity Assessment*; SAGE, Publications Ltd: Thousand Oaks, CA, USA.

¹⁰⁸ Shore J. (2022) *Data Incoming: How to Close the Cyber Data Gap*, War on the Rocks, October 18, available at <https://warontherocks.com/2022/10/data-incoming-how-to-close-the-cyber-data-gap/>.

¹⁰⁹ Eriksson J. & G. Giacomello, (2022) "Cyberspace in Space: Fragmentation, Vulnerability, and Uncertainty" in *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation* edited by Myriam Dunn and Andreas Wenger, London: Routledge, pp.95-107.

(self) or something. Hence, if we focus on the 'object' that can be damaged or hurt, we may develop valid indicators of 'security' so that relevant cybersecurity policies could be developed by all relevant actors.

Focusing on *conflicts* is one of the preferred choices when it comes to data and especially if the "agents" are actual governments. Governments, at all levels (national and local) are not the only but certainly one of the most essential actors when it comes to developing cybersecurity policies. Nonetheless, the focus of conflicts, even when the available data is rather large,¹¹⁰ is quite unsatisfactory for developing effective policies and moderately interesting to understand the motives and actions of sovereign government actors. This consequence is due to the **granularity**¹¹¹ of the data, which in the case of data on interstate-conflicts is not enough well defined and it proves to be quite *generic*.

For example, even the very large database GDELT (<https://www.gdeltproject.org/>) on global events collected from an extremely large number of media sources, while more than adequate for academic research and papers, ultimately, it comes out as too broad and generic if it has to function as main basis to develop comprehensive cybersecurity policies. This report has a strategic positioning (if we can say it) in the sense that it looks at the overall picture, the macro-level to develop **templates** for cybersecurity policies. Inevitably a wholesome approach to the security of cyberspace would have to entail security policies for *human users*, who often are the weakest link in cybersecurity.¹¹² It is quite challenging, but we aim at combining both the levels of (a) human users (b) and government actors.

The technological advancements observed over the last decades now affect all aspects of our lives. One of such evolutions is the quantity of new data produced every day: huge amounts of data are being generated every second from multiple sources, including electronic and, more in general, digital devices. Social media interactions or any other kind of tracked activity, together with the availability of digital documents represent examples of data sources that did not exist 20 years ago. Getting access to such data lakes has opened new opportunities for social scientists changing some of the paradigms

¹¹⁰ Christopher Whyte et al. (2018) "Rethinking the data wheel: Automating Open-access, Public Data on Cyber Conflict", Conference Paper · May 2018 10th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn, at <https://www.researchgate.net/publication/326276276>.

¹¹¹ Bettini, C., Dyreson, C. E., Evans, W. S., Snodgrass, R. T., & Wang, X. S. (1998) "A glossary of Time Granularity Concepts", *Temporal databases: Research and practice*, pp. 406-413.

¹¹² E.g. Eric Rutger Leukfeldt (ed.) (2017) *Research agenda. The Human Factor in Cybercrime and Cybersecurity*, May, Den Haag: Eleven International Publishing.

of the past. If properly treated and analyzed, such data can be a powerful instrument of information to improve our knowledge about specific arguments of interest in social sciences.

One of the traditional missions of sociologists and political scientists, as social scientists, has been to explain what happens when new elements, such as huge volume of data, impact upon societies. Thanks to the “wealth” provided by Big Data (BD), also Artificial Intelligence-related social research, such as in the legal sector, in electoral studies, political communications or in defense analysis is exploding. It is, however, in the availability and possibility of analyzing much larger quantities of data, that lays the path to better methodology in the social sciences, which is, incidentally, the only alternative for disciplines that cannot rely extensively on the experimental method. Computer and computer networks are no strangers in the social sciences of course, and indeed there has been a much larger interest for them by social/political scientists especially after the advent of the internet. The field of communications has, of course, been at the forefront, followed by sociology. In addition to the comprehensible expectations for the positive consequences that Big Data will have on the various fields of social sciences, first and foremost in cybersecurity. Overall, there are currently at least two principal disciplines that try to merge computing and the social sciences, namely **computational social science** and the more recent (thanks to social media data) social computing.¹¹³ The teaching experience examined in this paper belongs to the latter discipline, as the authors think that, when it comes to entering the job market for political science students may be more competitive in those skills related to social media and human-computer interactions.

The appreciation that high quality data frames (HQD) --particularly in an era of Big Data and Large Language Models (LLMs)-- have become of strategic importance for governments and corporations worldwide is widely shared. The HQD has demonstrated to be one of the most transformative human-build forces in the current days. These elements will be central for this part of the overall research. The ultimate goal, as we indicated above, is to procure/create better quality, more precise datasets and database

¹¹³ See for example David Lazer et al. (2009) “Life in the network: the coming age of computational social science” *Science*. February 6; 323(5915): 721–723. doi:10.1126/science.1167742 or Eugene Ch’ng (2014) “The Value of Using Big Data Technologies in Computational Social Science”, 3rd ASE Big Data Science Conference, Tsinghua University Beijing, 3-7 August 2014.

that could provide a more **reliable** and **validated**¹¹⁴ basis to develop national and international cybersecurity policies.

Reliance on big data has generated both extensive social benefits and widespread concerns, from enforcing automated disinformation campaigns, using mainly bots able to spread millions of tweets across the Internet and meddling in foreign elections to training AI systems in order to identify premature signs of cancer and therefore permit for more targeted precise medical treatments. As expected, the TQD system and the complex algorithms which might derive from the former started to be extensively incorporated in the sphere of military affairs. Military development and production of autonomous or semiautonomous vehicles, based on millions of coding lines, have become key elements in fighting terrorist networks and near-peer competitors, therefore minimizing the risk of human casualties. Conduct cyber attacks by manipulating adversary's data or developing breach risk predictions by analysing one's own IT asset inventory has also become advanced tactics to defend or attack physical and non-physical infrastructures.

The application of the HQD and AI are currently allowing these technologies to claim a status quo position among other high-tech innovations. It does not come with a surprise, consequently, that a global competition has emerged between United States, China and Europe, Advanced state economies and even private firms claim to lead such race or some of her aspects, with the final goal to shelter a competitive advantage which might shape the next decades of "Great Power" competition.

Clearly, foreign antagonisms between states and domestic rivalries between private businesses are not the only features concerning the efficient exploitation of big data and AI systems. New questions arise about data sharing within private institutions and between state departments. The academic literature has shown already cross-departments jealousies in the private sphere and interservice rivalries between different branches of a country's armed forces. The American Department of Defence (DOD) has underlined the critical importance and eventual problematics of making data accessible and interoperable among various branches of the DOD, but not, for example, towards

¹¹⁴ As it is well known, *validity* and *reliability* are the two *most important* attributes when it comes to datasets. While reliability concerns "the extent to which [...] any measuring procedure yields the same results in repeated trials", validity pertains to "the crucial relationship between concept and indicator". Both are, nonetheless, a "matter of degree". See Carmines, Edward G. & Richard A. Zeller. 1979. *Quantitative Applications in the Social Sciences: Reliability and validity assessment*. Thousand Oaks, CA: SAGE Publications Ltd and Trochim, William M. 2006. *The Research Methods Knowledge Base*. 2nd Ed. Version, at <http://www.socialresearchmethods.net/kb/>.

other US intelligence agencies. The Pentagon started to advocate and implement standard data formats, machine-to-machine communications and strengthen cross-department data loss prevention systems.


Former Secretary of Defense, David Norquist, for example, and his successor Kathleen Hicks both share the same position on data sharing, claiming that “any DOD data is a resource for the whole agency”. The new Digital Modernization program adopted by the DOD – which has the broad scope to move the department from simple automation to AI algorithms, allowing much more time saving and better decision making processes – passes its success through the vast flows of data in need to be standardized across all the branches of the Pentagon. If AI, training HQD, cloud storage, 5G and others are the technologies of the present, the ground-breaking and the next step in the high-tech realm might find its answer based on physics and new technologies such as quantum mechanics and quantum computing. This emerging playing field could revolutionize and speed up information processing by “hundreds of years” and confer significant economic and national-security advantages to countries and businesses that dominate it.

As we indicated in the introduction, developing cybersecurity policies has been heavily affected by (among other things) : (1) lack of publicly available data on cyber capabilities and surrounding proxies in Cyberspace, (2) simplification and (3) capturing the “duality” (i.e. offense and defense) of cyber capabilities, (4) the problem of attribution, (5) difficulties in linking different sources of data. In the next sections of this report, the authors believe that it is more convenient for the reader to be exposed to the methodology used, before being exposed to the outcome of the experience, which will come after the section on the methodology.

1.2 A Glance at the Various Actors

Cyber security represent a research field that has been studied under a wide range of perspectives. Among many topics that have been widely studied in the field of **cyber security**, strangely enough, the evaluation of cyber power represents a topic that has not received significant attention in current literature.¹¹⁵ Cyber power can be defined by

¹¹⁵ See for example Gorwa, R. & M. Smeets (2019) "Cyber conflict in political science: a review of methods and literature", paper presented at the ISA Annual Convention Toronto, March 2019, available at https://scholar.google.com/scholar?hl=it&as_sdt=0%2C5&q=Gorwa+and+Smeets+%282019%29&btnG=.

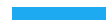


the interactions of both state and non-state actors within the contemporary international political landscape. One possible reason for such an oversight may be attributed to the elusive nature of cyber power compared to other dimensions of power, making it difficult to encapsulate within a precise cause-and-effect analytical framework. Unlike other forms of power, it is challenging, for instance, to argue that an increased number of unattributable attacks definitively corresponds to a clear acknowledgment of 'coercion' or power politics.

Existing research has primarily focused on analyzing cyber power from a qualitative standpoint, providing frameworks for understanding its nature or proposing categorizations for this instrument of power. Alternatively, some studies have explored the concept of cyber power in relation to its extension of military power. However, while acknowledging that cyberspace has at times accelerated the erosion of state sovereignty, this analysis still emphasizes the significance of states as influential actors in the international system. In the realm of international politics, states continue to play a vital role in national security and international relations, utilizing various forms of power, including cyber power, to pursue their interests. Although the debate regarding whether cyberspace represents a new dimension of global politics continues among experts, there is substantial evidence of tangible actions carried out through malicious cyber tools. The lack of empirically structured analyses on the actual behavior of states in cyberspace highlights a limitation within academia and among experts. Qualitative analysis remains the predominant approach in this field, and researchers and experts face challenges in exploring alternative quantitative approaches. However, there is a noticeable absence of a comprehensive quantitative analytical framework capable of categorizing and quantifying cyber attacks aimed at achieving political objectives, launched or sponsored by states.

Despite these constraints, we have made efforts to adopt a quantitative approach that allows us to identify the main characteristics of cyber attacks by utilizing available databases from four distinct sources. Our ultimate aim is to categorize the methods, objectives, and other key features of relevant actors in this context. We do not question the existence of cyber power; rather, the focus is on understanding how cyber power compares to other forms of power. A comparative approach facilitates the classification


The preferred (and probably only) methods tend to be bibliometric and literature reviews, which, while suitable for writing academic papers in international relations and political science are insufficient and too broad to represent the basis for developing effective cybersecurity policies.



of when, where, and how cyber power is employed, while also enabling a quantitative assessment of the degree of superiority, inferiority, or equality within the cyber domain. Five prominent state actors, namely China, Russia, the United States, North Korea, and Iran, have particularly demonstrated cyber power. These countries are widely acknowledged as significant cyber actors in the international system. The Russian Federation strategically incorporates the cyber dimension into its national strategy, particularly in the context of hybrid warfare. Cyber assets play a crucial role within its strategic arsenal, serving various purposes such as cyber espionage, cyber attacks, botnets, and cybercrimes. The activities of these actors are pivotal in assessing the potential threats they pose to overall cybersecurity.

In contrast, North Korea and Iran have a different approach to cyber dynamics. They see themselves as being at a lower level in the international system compared to the U.S., Russia, and China. These two countries use cyber tools for both external and internal political goals. They also use these tools to generate funds to support their regimes, with the aim of bypassing economic sanctions imposed by the international community. It is believed that North Korea and Iran not only serve as origins of numerous hacking attacks, but they also sponsor attacks that come from other countries.

On the other hand, the People's Republic of China has several distinct characteristics. First, China plays a significant role in state-sponsored cyber-attacks. Over the years, it has become a dominant actor in the region, challenging the power of the United States across a vast geographical area. Additionally, China is compelled to invest in both cyber defense and offense capabilities due to its physical and digital infrastructure far surpassing that of Russia, Iran, and North Korea. Importantly, the competition between Washington and Beijing over the past three decades has transformed Beijing into a central hub for cyber technology research. This transformation is evident in the significant development of cyber capabilities. The initial phase of the research will focus on establishing a framework that enhances our understanding of qualitative aspects related to cyber power and how it should be interpreted in international politics. This section aims to quantify the use of cyber power in interactions involving both states and non-state actors. The objective is to empirically measure and validate the assertions made through data analysis. Methodologically, a quantitative data analysis is conducted to evaluate the actual deployment of cyber power, particularly in the context of cyber-attacks, for the five cases examined: the United States, China, Russia, Iran, and North Korea.



Using a quantitative analysis is appropriate for analyzing these scenarios because it provides an objective and data-driven perspective. This approach allows for the identification of patterns, trends, and correlations in the behaviors of state actors involved in cyber-attacks. It also enables the examination of interactions between state and non-state actors. While this approach allows for the collection of empirical evidence and testing of research hypotheses, suited for scholarly research, we describe it here only as a *benchmark*, to show the level of available evidence that is today (in the best circumstances) used as leading markers for governments (and sometimes the private sectors as well) to produce cybersecurity policies and regulations.

1.3 Examples Data collection and structures

In the initial phase of the research we have had several discussions on establishing an epistemological and ontological framework that enhances our comprehension of qualitative aspects related to 'what is' cyber power and 'how' it should be interpreted within the dynamics of international politics. Adopting a quantitative analysis may be deemed appropriate when analyzing these scenarios because it offers an objective perspective that is driven by data. This approach enables the identification of patterns, trends, and correlations in the behaviors of state actors involved in cyber-attacks. Due to its inherent nature, quantitative analysis facilitates the identification of prevalent patterns, such as the most frequently targeted types of targets in cyber attacks, the preferred attack techniques, periods of heightened activity, and potential relationships between attacks and the political contexts in which they occur or originate. It also allows for the examination of interactions between state and non-state actors.

We considered that a **quantitative approach** would allow for the utilization of cluster analysis, which can help shed light on the relationships between various variables or entities. Based on these considerations, data spanning from 2000 to 2023 has been collected and subsequently organized into a comprehensive dataset. The data used for our analysis are not only aggregated but also facilitate a specific vertical analysis on the phenomenon of Advanced Persistent Threats (APTs). The dataset primarily focuses on data related to the volume of cyberattacks, their success rates, temporal concentration, and the diversity of actors. The substantial quantity of data (approximately 11,000 events examined), coupled with the valuable information contained within, can be leveraged to identify regularities, discover trends and patterns regarding the behaviors of both state

and non-state actors in cyberspace. Ultimately, this can provide highly useful empirical evidence on the utilization of cyber power by the actors under scrutiny.

With a particular reference to this study/research, a quantitative approach allows to carry out cluster-analysis that eventually can be employed to shed light on the relational analysis among various variables or entities. Starting from these considerations, data spanning the period from 2000 to 2023 has been collected and later organized in a comprehensive dataset. The data used for our analysis are not only aggregated but also facilitate a specific vertical analysis on the phenomenon of Advanced Persistent Threats (APTs). The dataset focuses mainly on data relative to the volume of cyberattacks, their success rates, temporal concentration, and the diversity of actors. The substantial quantitative volume (approximately 11,000 events examined), coupled with the precious information contained in these data, can be leveraged to identify regularities, discover trends and patterns relative to the behaviors of both state and non-state actors within cyberspace, that, ultimately, can provide extremely useful empirical evidence on the deployment of cyber power by the surveyed actors. The dataset used for the analysis is derived from four existing databases (the latter two are also the basis for Table 1 included down below):

- EuRepocData
- Council on Foreign Relations
- Mitre ATT&CK
- APT Groups and Operations database

Usually, the reasons to focus on building datasets such as the one below more precisely include:

- Data availability: the databases taken into considerations provided substantial amounts of data collected from a variety of sources and sectors. In total, the database contains about 11,000 cyber-attacks events.
- Data quality: These data demonstrate reliability and high quality. According to the documentation, the databases have been constructed in adherence to stringent standards in terms of data collection, data organization, and, finally, data validation. In addition to ensuring a minimal risk of incurring into errors, this process fosters confidence in the validity of the results obtained.

- Wide temporal coverage: the time frame of selected databases stretches over more than two decades (from 2000 to 2023), facilitating a comprehensive, long-term analysis and the examination of trends over time.
- Opportunities for correlation and intricate analyses: The selected databases yield itself to conducting complex statistical analyses, including correlation and other statistical modeling. This approach allowed for the exploration of relationships or behavioral patterns that may be challenging to discern through qualitative research methods.

Among many data dimensions, of particular interest are features like the one in the list belows or with some similar terminology:

1. **Title:** A concise description of the cyber attack;
2. **Date:** The date, corresponding to the initiation of the attack;
3. **Year:** The specific year of the cyber attack;
4. **Type (of attack):** Specifying the nature of the attack (Data Theft, Sabotage, Espionage, etc.);
5. **Description:** Offering a detailed description of the cyber attack;
6. **APT:** Identifying whether the attacks are classified as Advanced Persistent Threats;
7. **Affiliations:** Listing the affiliations of the perpetrators involved in the examined cyber attacks;
8. **Sponsor:** Indicating the responsible country (from the five surveyed) for the attack, information previously confirmed by the databases used as sources;
9. **Victim Category:** Defining the position held by the victim entity within society (institution, company, etc.);
10. **Affiliation Category:** Determining whether the state government listed as the initiator of the attack is indeed responsible, according to the sources provided by the databases.

Among these data features, we would like to highlight the 'Affiliation Category' as it serves to establish whether the examined attacks can be attributed to a state actor. Establishing whether these threats can genuinely be associated with state responsibility represents an extremely useful information for the objectives of this analysis. Note that this category is the outcome of additional processing and refinement of the data within the dataset. It

involves cross-referencing evidence and patterns related to Advanced Persistent Threat (APT) groups, as well as the objectives and targets of cyber attacks.

In addition, a new variable can be created by aggregating affiliation category based on whether the actor can be classified as a **Governative** vs **unknown one**. This categorization is particularly useful because it facilitates conducting more in-depth quantitative analysis. When it comes to data transformation process, the first step regarded the merge of the four databases making sure the consistency of the data across them. Next, as briefly explained above, ten dimensions has been selected among many other data variables available and organized in pre-selected categories.

When it comes to data transformation process, the first step regarded the merge of the four databases making sure the consistency of the data across them. Next, as briefly explained above, ten dimensions has been selected among many other data variables available and organized in the pre-selected categories previously described. The final dataset is comprised of about 11'000 data points. The large amount of data, though in relative terms, made it convenient and statistically sound to carry out a series of statistical analysis.

Descriptive statistics is always used at the beginning to gain a better understanding the various fundamental aspects characterizing the phenomenon of the cyber attacks, including, but not limited to, the distribution of different typologies of cyber attacks as well as grouped by the country of origin; the distribution of Advanced Persistent Threats (APTs). It is usually followed by cross-country statistical analysis in order to discern the specificities of cyber actions put in place by each country, highlighting shared techniques as well as different strategies adopted by each of them. Such a comparative analysis across countries has enabled us to significantly enhance our understanding of the capabilities of the selected nations in the cyber space. In general, Python is the main software tool used to perform the above-mentioned statistical analysis. This analytical approach should be designed to address particular inquiries related to cyber attacks. Specifically, such analysis would consider the *political dimension of cyber power*, operating under the assumption that states are broadening their interpretation of power in cyberspace. They view this environment as a valuable asset for achieving full-spectrum dominance across multiple domains and targets, surpassing the simple objectives of destroying and disabling adversary infrastructure.

Another example of valuable use of available data is also based on the 2013-MITRE developed 'ATT&CK®', the (freely) accessible knowledge base of adversary tactics and techniques, based, as the organization indicates, 'on real-world observations' (see the previous example). The National Institute of Standards and Technology (NIST) sponsored the National Cybersecurity FFRDC (NCF) one of the six 'Federally Funded Research and Development Centers' (FFRDC) now managed by MITRE. The NIST is, in itself, one of the best known (and respected) sources of research on cybersecurity.

On the MITRE Web site it is also possible to find a basic description of the dataset: the 'MITRE ATT&CK® is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.' The specific dataset used for this work is labelled 'Groups', where groups "are activity clusters that are tracked by a common name in the security community". An abridged version of the table used in the paper attached in Appendix 1 is the Table 1 presented below.

Table 1 – A extraction of the available dataset of the cyber attacks (Source: Giacomello, Iovanello and Martino, 2023; see Appendix 1).

ID	name	Industry	Origin	Target 1	Target 2	Target 3	Target 4	Target 5	Target 6
G0099	APT-C-36	government	South America	Colombia					
G0023	APT16	government	China	Japan	Taiwan				
G0025	APT17	government	China	U.S.					
G0016	APT29	government	Russia	North America	Europe	Asia	Middle East		
G0016	APT29	telecoms	Russia	North America	Europe	Asia	Middle East		
G0016	APT29	high-tech	Russia	North America	Europe	Asia	Middle East		
G0016	APT29	media	Russia	North America	Europe	Asia	Middle East		
G0022	APT3		China						
G0013	APT30		China						
G0050	APT32	government	Vietnam	Vietnam	Philippines	Laos	Cambodia		
G0050	APT32	media	Vietnam	Vietnam	Philippines	Laos	Cambodia		
G0064	APT33	energy	Iran	U.S.	Saudi Arabia				
G0067	APT37		North Korea	South Korea	Japan				

ID	name	Industry	Origin	Target 1	Target 2	Target 3	Target 4	Target 5	Target 6
G0117	Fox Kitten	energy		Middle East	North Africa	Europe	Australia	North America	
G0117	Fox Kitten	IT		Middle East	North Africa	Europe	Australia	North America	
G0117	Fox Kitten	manufacturing		Middle East	North Africa	Europe	Australia	North America	
G0101	Frankenstein								
G0093	GALLIUM	telecoms	China						
G0036	GCMAN	finance							
G0115	GOLD SOUTHFIELD								
G0084	Gallmaker	defense		Middle East					
G0084	Gallmaker	government		Middle East					
G0047	Gamaredon Group	government		Ukraine					
G0078	Gorgon Group	government	Pakistan	U.K.	Spain	Russia	U.S.		
G0043	Group5	individual	Iran	Syria					
G0125	HAFNIUM	defense	China	U.S.					
G0125	HAFNIUM	government	China	U.S.					
G0126	Higaisa	government	South Korea	Poland	North Korea	China	Japan	Russia	
G0072	Honeybee	NGOs		Argentina	Vietnam	Canada	Singapore	Japan	Indonesia
G0100	Inception	government		Russia	U.S.	Europe	Asia	Africa	Middle East
G136	IndigoZebra	government	China	Central Asian					
G0119	Indrik Spider	finance	Russia						
G0004	Ke3chang	defense	China						
G0004	Ke3chang	government	China						
G0004	Ke3chang	energy	China						
G0094	Kimsuky	government	North Korea	South Korea	U.S.				
G0032	LazarU.S. Group	media	North Korea						
G0077	Leafminer	finance	Iran	Middle East					
G0077	Leafminer	government	Iran	Middle East					
G0065	Leviathan	infrastructure	China	U.S.	Europe	Canada	South Asia	Middle East	
G0065	Leviathan	aereospace	China	U.S.	Europe	Canada	South Asia	Middle East	
G0065	Leviathan	healthcare	China	U.S.	Europe	Canada	South Asia	Middle East	
G0065	Leviathan	defense	China	U.S.	Europe	Canada	South Asia	Middle East	

ID	name	Industry	Origin	Target 1	Target 2	Target 3	Target 4	Target 5	Target 6
G0065	Leviathan	government	China	U.S.	Europe	Canada	South Asia	Middle East	
G0030	LotU.S. Blossom	government		Southeast Asia					
G0095	Machete	defense	Spain	Latin America	U.S.	Russia	Europe		
G0095	Machete	telecoms	Spain	Latin America	U.S.	Russia	Europe		
G0095	Machete	government	Spain	Latin America	U.S.	Russia	Europe		
G0059	Magic Hound	defense	Iran	U.S	Middle East				


Table 1 presents just a section of a larger dataset. Despite the (relative) size of the dataset (almost 200 observations) and the undeniable quality, it is still a small basis for understanding cyber-attacks and thus it is quite a challenge to produce viable cybersecurity policies until the problems we have discussed thus far, namely the size of datasets available and the quality of data, are addressed and possibly resolved.

2 Possible Alternative: Synthetic Data?

Less than a decade ago, *The Economist* suggested that data is the new oil. After many years, it can be acknowledged that, as seldom happens, the prediction was correct. As research has widely acknowledged, data availability in the filed cyber security remains an issue. This is true in relative terms, compared to various forms of cyber-attacks that are estimated to occur globally, based on real negative effects provoked. It is well known that only a small portion of cyber-attacks are detected worldwide. What is more concerning for research is the fact that the quantity of data that provide information describing the entities involved in a given cyberattack, together with its characteristics, methods of operation, adopted tools, timing etc. remain extremely limited even in absolute terms. To have a better idea of the phenomena, in the social sciences, a dataset consisting of around 300 observations is considered to be of adequate size.

Therefore, cyber security suffers particularly from data constraints. While data availability is limited, however, synthetic data can play a crucial role in addressing this challenge. Indeed, synthetic data are being used in a variety of fields and for a series of purposes¹¹⁶.

¹¹⁶ Hradec, J., et al. (2022) Multipurpose synthetic population for policy applications, EUR 31116 EN, Publications Office of the European Union, Luxembourg, doi:10.2760/50072, JRC128595.



In contrast to data collected in the real world, synthetic data is derived from a process that generates data artificially, in the sense that it does not refer to actual observations. Starting from real data, synthetic data generators are able to create data with the same characteristics of the original one. In other words, synthetic data can have the same statistical properties of the real data they have been trained on.

Synthetic data are created through a model, typically with the intention of substituting real data. By overseeing the data generation process, users have the ability to regulate the extent of private information disclosed by synthetic data and manage its similarity to authentic data.

Synthetic data is being used in a wide range of domains, as it has been proved to be helpful for a variety of tasks. The most important use-cases identified can be summarized into three main groups:

- Privacy Protection
- Data augmentation
- Bias mitigation

(1) Data privacy represents a major concern for many institutions. So much so that the European Union, first, followed by US institutions, have regulated the use of private data by approving the GDPR. GDPR regulation imposes public or private companies, institutions, or any other subject that enters into possession of personal data, to respect a set of rules regarding their use and treatment.

One of the main concerns of data privacy is to ensure data anonymity in such a way that it is impossible to trace back to the individual starting from collected data. This becomes even more impeding when sensitive data such as health and wealth data are involved.

In the context of cyber-security specifically, data privacy matters in consideration of the effective risk the companies and/or institutions subject to cyber-attacks being identified, with all the implications on companies' reputation that this might cause. As a result, targeted subjects are reluctant to disclosing this information. Hence, applying techniques that make sure the anonymity is of crucial importance.

(2) In addition, as already mentioned, analyzing cyber security from a quantitative perspective with the aim of extracting patterns is hindered also by the limited amount of data available. The lack of cyber data is pervasive to the field. Though there are a number of reasons contributing to this, the main cause of data constraints can be attributed to objective difficulties *to capture the features of the cyber-attacks for their own nature*. To succeed, attackers should conceal their identity by adopting a series of techniques that help them conceal their characteristics.

The problem of working with small samples of data is that limited size samples do not lend themselves to applying statistical techniques and methods, as statistics, intended as a scientific discipline, needs sufficiently large enough samples of data. In this context, data augmentation can play an important role in overcoming such an issue by generating new synthetic datasets while preserving the properties of the original data.

(3) Furthermore, it is acknowledged that collected data are frequently biased for a number of reasons that goes beyond the scope of this report. Just to mention a few, however, these biases include historical, gender, religious, social, economic and any other aspects in which, unfortunately, biases do exist not only throughout history but also in our everyday lives. It is not surprising, therefore, that any samples of data extracted within such context most probably is affected from the same biases. Recognizing such an issue, however, allows researchers to address it as statistical techniques offer a means to tackle similar problems.

Apart from these, synthetic data can also provide a valuable contribution to mitigate biases by generating information inherently immune to biases by construction. It is also worth noting that, in general, small-sized datasets are more prone to embody any kind of skewness in their distribution.

This last consideration, in particular, leads to the following question: what are some their most important properties and how are synthetic data generated? The short answer is that synthetic data are as good as they resemble the same properties of the real data. They should be able to display the same statistical properties of the original data, and thus to capture almost the full spectrum of the patterns present in the underlying population. In general, synthetic data are generated by Machine Learning (ML) or Deep Learning (DL) models which have been previously trained to learn the task of generating data similar to the available ones. For tabular data in particular, these models are based

on classifiers, such as Vector Machines, Inverted-Decision Trees and Random Forest.¹¹⁷ Last but not the least, we are quite aware that synthetic data present also several limitations. Therefore, one should handle them with caution and use them only after passing several tests ensuring their fairness and reliability.

3 Future Directions of the Research

3.1 Where we are now

The overall goal that this section (4.1) of SERICS7-EcoCyber is tasked with is to explore and analyze national and international policies of cybersecurity. As showed in the introduction, the quality and effectiveness of such policies go from mixed to problematic. Malicious actors go to extreme lengths to obscure their identities and where they operate from and they are, for most part, quite successful. Moreover, if such actors operate as “state-sponsored” their requirement is to achieve *plausible deniability*, namely that their government-sponsors should be able to deny, in front of international media as well as international law, that they have nothing to do with attacks and breaches into computers, networks, databases and infrastructures. This “minimum” requirement is fairly obtainable (plausible deniability in international law does not require particularly high standards). Clearly, as long as this state of affairs persists, cybersecurity policies will face a steep, uphill battle to be more effective and actually help protect the cyber-perimeters of companies, governments and users.

To produce better, more effective and useful cybersecurity policies is undoubtedly possible via improvements in various areas, as for example clearly indicated in this report by the UniMI team. Another essential contribution is to strengthen the bases on which such policies rest, that is the data that the policies rely on to suggest the necessary changes and implements. To increase the quality of such data is necessary (1) to take a “picture” of the present situation and what is currently available (where we are now) and (2) find ways/methods to improve and refine the data quality.

There would be, of course, diverse strategies to achieve such goal; however, as we reported in the previous section, we strongly believe that synthetic data and Large

¹¹⁷ Jordan, L. et al (2022) “Synthetic Data -- what, why and how?”, pre-print, arXiv:2205.03257 [cs.LG].

Language models may offer one of the best tools to foster data quality and thus the quality and effectiveness of cybersecurity policies in the future.

3.2 Where We Go From Here

As of November 2023, on the AI community platform *Hugging Face* (<https://huggingface.co>) there are more than 325.000 pre-trained OS-LLMs. A selection of some of these models could be used for fine-tuning using better quality cybersecurity data. Likewise, there are several APIs that offer work on synthetic data (e.g. Gretel at <https://console.gretel.ai/login> or Mostly at <https://mostly.ai>) as well as YouTube tutorials (<https://youtu.be/e0I9sHnPIDc?si=zA33MZSycn2x7Yxh> or <https://youtu.be/HIusawrGBN4?si=7M6lIRekrcaX72kb>). The offer and opportunities have “exploded” in the last 12 months, namely since OpenAI launched ChatGPT in November 2022. Not all of what is available is useful or even helpful and it is necessary to proceed with testing different alternatives.

Thus far, we have continued the work towards the development of a modeling framework based for the analysis of threat actors/agents using network analysis methodology and identifying potential data sources. We are now discussing the future application of Open Source (OS) Large Language Models (LLMs). We are now considering some of the models now available and preparing to test which is the most suited for our analysis. The purpose of such move is to speed up the process of examining the largest possible number of documents that may yield data that can then be used to direct the development of national/international cyber-security policies.

As we indicated above, synthetic data, LLMs and higher quality data are not the panacea for all the issues included in the concept of cybersecurity, far from it. It could, nonetheless, represent a considerable leap in developing cybersecurity policies more effective and adaptable to contrast the growing number of malicious actors (both non-state and government-sponsored) their increasingly sophisticated tools.

Appendix 1

Giampiero Giacomello, Antonio Iovanella, Luigi Martino (2023), "A Small World of Bad Guys: Investigating the Behavior of Hacker Groups in Cyber-Attacks", pre-print on arXiv (submitted for peer-review) available at:

<https://arxiv.org/abs/2309.16442>