LA COMUNITÀ INTERNAZIONALE

Rivista Trimestrale della Società Italiana per l'Organizzazione Internazionale

QUADERNO 29

Cybersecurity Governance and Normative Frameworks: Non-Western Countries and International Organizations Perspectives

Edited by
Pietro Gargiulo, Davide Giovannelli, Annita Larissa Sciacovelli

With a preface by
Riccardo Sessa and Mart Noorma

EDITORIALE SCIENTIFICA
Napoli

LA COMUNITÀ INTERNAZIONALE

RIVISTA TRIMESTRALE DELLA

SOCIETÀ ITALIANA PER L'ORGANIZZAZIONE INTERNAZIONALE

QUADERNI (Nuova Serie)

29

SOCIETÀ ITALIANA PER L'ORGANIZZAZIONE INTERNAZIONALE

CYBERSECURITY GOVERNANCE AND NORMATIVE FRAMEWORKS: NON-WESTERN COUNTRIES AND INTERNATIONAL ORGANIZATIONS PERSPECTIVES

Edited by
Pietro Gargiulo, Davide Giovannelli, Annita Larissa Sciacovelli

With a preface by
Riccardo Sessa and Mart Noorma

EDITORIALE SCIENTIFICA
Napoli

This publication was financed by the
NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)

Manuscripts have been subjected to a peer review process prior to publication

Via San Biagio dei Librai, 39
89138 - Napoli
ISBN 979-12-5976-999-2

SUMMARY

PREFACE – RICCARDO SESSA, MART NOORMA ……..…….....1

INTRODUCTION – DAVIDE GIOVANNELLI ……..……..……...….3

GENERAL ASPECTS

ANNITA LARISSA SCIACOVELLI – Malicious Cyber Operations Committed by States and Non-State Actors: The International Legal Landscape ….……...…….…..7

SEBASTIANO LA PISCOPIA – The Regulatory Relevance of the Fifth Domain's Weapons Definition ……..…….…….....35

NON-WESTERN COUNTRIES PERSPECTIVE

ARINDRAJIT BASU, BHARATH GURURAGAVENDRAN – Unveiling India's Strategy: Navigating International Law and Indian State Practice on Security Operations ……..…….…….....67

KEIKO KONO – Japanese Regulatory Framework on Cyber Operations and Cybersecurity: Ambition Toward More Active Posture …….…..…..…….109

TAL MIMRAN, LIOR WEINSTEIN – The Need for Oversight on Surveillance Technologies: A (Painful) Perspective from Israel ……141

ISAAC MORALES TENORIO, MARIANA SALAZAR ALBORNOZ – Normative Framework, Decision-Making and Responses to Cyber Operations: A View From Mexico ……...……...…181

INTERNATIONAL ORGANIZATIONS PERSPECTIVE

PIETRO GARGIULO – United Nations and Cybersecurity ……..……203

IVAN INGRAVALLO, ELENA DRAGO – The Council of Europe's Actions in the Field of Cybersecurity ……..……..…….....217

ELISA TINO – Cybersecurity in Southeast Asia: What is ASEAN Doing? ……229

MARCO FASCIGLIONE, MICHELE NINO – The Activity of the Organization of American States in the Field of Cybersecurity ……..…249

ANTONIO MARICONDA, PIERFRANCESCO ROSSI – The Shanghai Cooperation Organization and Cybersecurity: A Sino-Russian Approach to International Law? ……..…….…….…….....265

SILVIA VENIER – The Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace ……..…….…….…….....291

THE AUTHORS

ANNITA LARISSA SCIACOVELLI – Professor of International law, University of Bari Aldo Moro (Italy). Member of the Advisory Board, European Union Agency for Cybersecurity (ENISA). Member of the Defense Innovation Office, Chief of Defense Staff, Italian Ministry of Defense.

SEBASTIANO LAPISCOPIA – Colonel of the Italian Army. Former Head of the International Legal Affairs Office of the Italian Defense General Staff. Chief Editor of the review «Rassegna della Giustizia Militare», Italian Ministry of the Defense.

ARINDRAJIT BASU – PHD Candidate at the Leiden University, Faculty of Global Governance and Affairs. Digitalization and Human Rights Research Consultant with the United Nations Development Program (UNDP). Previously, Research Lead at the Centre for Internet&Society.

BHARATH GURURAGAVENDRAN – Graduate student at New York University (NYU). Research Consultant with NYU's Centre for Human Rights and Global Justice. Previously, Assistant Professor at Jindal Global Law School; Legislative Assistant to Member of Parliament (through the LAMP Fellowship).

KEIKO KONO – Visiting Researcher at the Meiji University Cybersecurity Laboratory, Tokyo. Previously, Post-Doctoral Researcher, University of Copenhagen. Former Senior Research Fellow of Public International Law and Cybersecurity, National Institute for Defence Studies (NIDS), Japanese Ministry of Defence. Former law researcher of NATO CCDCOE.

TAL MIMRAN – Associate Professor, Zefat Academic College. Academic Director, International Law Forum of the Hebrew University. Fellow at the Federmann Cyber Security Research Center, Law Faculty, Hebrew University. Previously, Legal Adviser, Israeli Ministry of Justice.

LIOR WEINSTEIN – Master's student of International Law (LLM), Hebrew University, Jerusalem. Researcher in Law and Technology and International Law, Tachilit Policy Center. Member of the International Law Forum, Hebrew University, and of the Federmann Cyber Security Research Center – Cyber Law Program.

ISAAC MORALES TENORIO – Senior Director for Cybersecurity & Data Privacy, LATAM, FTI Consulting. Previously, First General Coordinator for Multidimensional Security Issues, Mexico's Ministry of Foreign Affairs. Coordinator for Multidimensional Security. Member of the UN GGE to Advance Responsible Behavior in Cyberspace; Chairperson of the OAS Working Group on Confidence-Building Measures in Cyberspace.

MARIANA SALAZAR ALBORNOZ – Professor of International Law, International Humanitarian Law (IHL) and International Criminal Law (ICL), Universidad Iberoamericana, Mexico City. Previously, Rapporteur for International Law Applicable to Cyberspace and for Privacy and Data Protection, Inter-American Juridical Committee, Organization of American States.

PIETRO GARGIULO – Professor of International Law, University of Teramo (Italy). Editor in Chief, "La Comunità Internazionale" ("The International Community"), Quarterly of the Italian Society for International Organization (SIOI).

IVAN INGRAVALLO – Professor of International Law, University of Bari Aldo Moro (Italy). Associate Editor, "La Comunità Internazionale" ("The International Community"), Quarterly of the Italian Society for International Organization (SIOI).

ELENA DRAGO – Women4Cyber Chapters Coordinator. MA Philosophy, Politics and Economics in MED, University of Bari Aldo Moro (Italy).

ELISA TINO – Associate Professor of International Law, University of Naples "Parthenope" (Italy). Author of monographs and scientific articles concerning the law of international organizations and some topics of public international law.

MARCO FASCIGLIONE – Researcher of International Law and Human Rights Law, Co-Director of the Business and Human Rights Summer School, National Research Council (CNR, Italy). Member of Mission Appeals Tribunal (MAT), NATO.

MICHELE NINO – Professor of International Law, University of Salerno (Italy). Holder of the Course of the Law Clinic in "International Protection of Human Rights", University of Salerno.

ANTONIO MARICONDA – PhD candidate in International Law, University of Naples Federico II. Research Fellow, University of Milan 'La Statale' on the project "Arms, Peace, and Sustainability" (ArPeSu). Author of scientific articles on both public and private international law, published in Italian and international journals.

PIERFRANCESCO ROSSI – Assistant Professor of International Law, Department of Political Science, University of Teramo. Adjunct Professor at Luiss University, Rome. His main research interests are the jurisdictional immunities of states, international organizations and diplomatic and consular agents, and the interaction between international law and domestic legal orders.

SILVIA VENIER – Research fellow in International Law, Department of Social and Political Sciences, University of Trieste.

MALICIOUS CYBEROPERATIONS COMMITTED BY STATE AND NON-STATE ACTORS: THE INTERNATIONAL LEGAL LANDSCAPE

ANNITA LARISSA SCICOVELLI

SUMMARY: 1. Introduction. -2. Threat actors in cyberspace: state and non-state actors. -3. Principal types of malicious cyberoperations: the ones whose effects fall below the use-of-force threshold. -4. Cyberoperations whose effects are above the use-of-force threshold. - 5. Technical and legal challenges in the attribution of cyberoperations to a state. - 6. The international responsibility of states for using criminal hackers to carry out cyberoperations. -7. Concluding remarks.

1. The recent exponential increase in malicious cyberoperations by both state and non-state actors is undermining national and international peace and security, and delicate geo-strategic balances[1]. This rise in threats in cyber space has become a critical global security issue, as highlighted in the "Concept Note for the Security Council of the United Nations" on "Maintenance of international peace and security: addressing evolving threats in cyberspace", of June 10, 2024[2], necessitating significant international attention from the international community.

---

[1] This publication is the result of the research conducted within the European Union co-financing-Next Generation EU: NRRP Initiative, Mission 4, Component 2, Investment 1.3 - Partnerships extended to universities, research centres, companies and research D.D. MUR n. 341 del 15.03.2022 –Next Generation EU (PE0000014-"SEcurity and Rights in the CyberSpace-SERICS"-CUP: H93C22000620001). On this topic see the contributions of H.S. LIN, *Offensive Cyber Operations and the Use of Force*, in *Journal of National Security Law and Policy*, 2010, 4; H. DINNISS, *Cyber Warfare and the Laws of War*, Cambridge, 2012, 74; M.N. SCHMITT, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, 2013; L. BAUDIN, *Les cyber-attaques dans les conflits armés*, Paris, 2014; M. ROSCINI, *Cyber Operations and the Use of Force in International Law*, Oxford, 2014; K. KITTICHAISAREE, *Public International Law of Cyberspace*, Cham, 2017; N. TSAGOURIAS, R. BUCHAN (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, Northampton, 2021; H. LAHMANN, *Unilateral Remedies to Cyber Operations*, Cambridge, 2020.

[2] See United Nations (UN) Security Council, Concept note for the Security Council high-level open debate on "Maintenance of international eace and sSecurity: Addressing Evolving Threats in Cyberspace", UN Doc. S/2024/446; Permanent Mission of the Republic of Korea at the UN, Arria-Formula Meeting on Cyber Security Evolving Cyber Threat Landscape and its Implications for the Maintenance of International Peace and Security, https://www.securitycouncilreport.org/. See in this book, GARGIULO, *The United Nations and*

Malicious cyberoperations are complex, committed with a high speed and technical sophisticated and they target - and sometimes severely impact - the information and communication technologies systems (ICTs) of private companies, public entities, and critical infrastructures within national cybersecurity perimeters[3]. These targets include, *inter alia*, healthcare systems, banking and financial services, large automated industrial complexes such as energy and manufacturing sectors, transportation, telecommunications (including satellites), and water plants, to cite a few.

Following the rapid evolution of digitalization after the Covid-19 pandemic, these entities and infrastructures have become essential for the regular functioning of governmental activities that provides essential civil, social, political, and economic services. Thus, malicious cyberoperations are a new form of intrusion into the sovereign prerogatives of states, making the protection of ICTs and the digital data stored in them crucial elements of national and international (cyber)security.

The aims of these malicious activities are to alter, degrade, destroy, or interrupt the correct functioning of ICTs, either partially or completely, and to alter, destroy or compromise, even irreversibly, the confidentiality, integrity, and availability of digital data that are essential for the cited services[4]. The impact of these activities is evident in both the digital and physical worlds.

These malicious activities are mainly transnational and are driven by the military, geopolitical, and financial interests of the various

---

Cybersecurity; S. LA PISCOPÌA, *The Regulatory Relevance of the Fifth Domain's Weapons Definition*.

[3] See the UN General Assembly resolution, *Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures*, December 23, 2003, n. 58/199, UN Doc. A/RES/58/199. See GEE, Report *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 14 July, 2021, UN Doc. A/76/135, para. 7, 14. See S. HAATAJA, *Cyber Operations Against Critical Infrastructure Under Norms of Responsible State Behavior and International Law*, in *International Journal of Law and Information Technology*, 2022, 423.

[4] See E.T. JENSEN, *Cyber Warfare and Precautions Against the Effects of Attacks*, in *Texas Law Review*, 2010, 88; O.A. HATHAWAY, *The Law of Cyber-Attack*, in *California Law Review*, 2012, 817; K. MAČÁK, *Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law,* in *Israel Law Review*, 2015, 55; M.N. SCHMITT, *The Notion of 'Objects' During Cyber Operations: A Riposte in Defence of Interpretive Precision*, ivi, 81; R. GEISS, H. LAHMANN, *Protection of Data in Armed Conflict*, in *International Law Studies*, 2021, 556.

actors acting in cyberspace, such as states and non-state entities[5]. Therefore, cyberoperations can be part of broader and complex strategies reflecting the states' agendas, potentially causing or exacerbating international crises and threatening international peace and security.

A notable example of such an operation is the cyber-attack on Viasat Inc.'s KA-SAT satellite, which disrupted Ukrainian civil and military communications just hours before the Russian military aggression on February 24, 2022[6]. This incident marks the Russian-Ukrainian conflict as the first to start in the cyber domain.

In the past, other hostile actions in cyber space were carried out, likely again by the Russian Federation, against Georgia in 2019, and against Ukraine during the Crimean War in 2014[7].

In this regard, the Council of the European Union (EU), in March 2022, adopted the *EU Strategic Compass for Security and Defense*, emphasizing that cyberoperations against European and Ukrainian network infrastructures were a significant part of Russia's hybrid

---

[5] Cyber space is made up of three segments: the first is physical and is made up of hardware systems and physical network infrastructures (computers, cables, servers); the other two segments are virtual and, specifically, one is composed of the software and other programs thanks to which the previous level can function, and the other consists of digital data that are stored in the hardware. For a definition of cyber space, see M.N. SCHMITT, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed., Cambridge, 2017, 564, and U.S. Dept. of Defense, *Law of War Manual*, 2023, 1025, according to which it is a «global domain within the information environment consisting of interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers». About the motivations behind cyberoperations see C. HEFFELFINGER, *The Risks Posed by Jihadist Hackers*, in *CTC Sentinel*, 2013, 32 ff; M. COHEN, F. CHUCK, G. SIBONI, *"Four Big "Ds" and a Little "r": A New Model for Cyber Defense*, in *Cyber, Intelligence, and Security*, 2017, 21 ff; F. DELERUE, *Cyber Operations and International Law*, Cambridge, 2020, 11 ff; NATO, *Summit of Warsaw Communiqué*, 2016, that states that «[T]he Alliance faces a range of security challenges and threats that originate (…) from state and non-state actors; from military forces and from terrorist, cyber, or hybrid attacks».

[6] See P.H. O'NEILL, *Russia Hacked an American Satellite Company One Hour Before the Ukraine Invasion. The Attack on Viasat Showcases Cyber's Emerging Role in Modern Warfare*, 2022, https://www.technologyreview.com; MICROSOFT, *Microsoft Digital Defense Report 2022, Russian State Actors' Wartime Cyber Tactics Threaten Ukraine and Beyond*, 41 ff; M. ORENSTEIN, *Russia's Use of Cyberattacks: Lessons from the Second Ukraine War*, in *Foreign Policy Research Institute,* 2022; J.A. LEWIS, *Cyber War and Ukraine*, 2022, https://csis-website-prod.s3.amazonaws.com.

[7] See G. NAKASHIDZE, *Cyberattack Against Georgia and International Response: Emerging Normative Paradigm of 'Responsible State Behavior in Cyberspace'?*, in *EJILTalk!*, 2020; P. ROGUSKI, *Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace*, 2020, www.justsecurity.org.

warfare toolkit, therefore the need to create an EU cyber defense policy[8].

Additionally, it is worth mentioning the cyberoperations against Albania in July and September 2022, allegedly conducted by Iranian hackers, aimed to completely shut down the government's ICTs and erase the digital data stored in them[9]. These cyber-attacks have been defined by the Albanian Prime Minister a state aggression and they prompted a statement from the North Atlantic Treaty Organization (NATO) on September 8, 2022, acknowledging them as state cyber aggression likely orchestrated by Iran[10]. Following the technical and legal attribution of these operations, NATO's Secretary General did not rule out invoking Article 5 of the North Atlantic Treaty, which pertains to collective defense actions to protect its member states[11].

These cases highlight the dangers of cyber weapons used also in conjunction with kinetic armed conflicts and underscore the importance of an analysis of the current complex landscape of threat actors, of the hostile activities in cyberspace, and of the international legal obligations of states.

Aim of this paper is to focus on cyberoperations during peacetime, and to serve as a preliminary foundation for the subsequent chapters of this book, which will explore both the normative frameworks and positions of non-Western countries in cyberspace, and the roles of international organizations in promoting common understandings, collaboration and international cooperation for the sake of an open, secure, stable, accessible and peaceful digital environment.

---

[8] See Council of the European Union, Strategic Compass for Security and Defense and for a European Union that Protects its Citizens, its Values and its Interests and Contributes to International Peace and Security, 2022, paras. 3, 5, 6, and 7; ID., *European Union Strategic Compass for Security and Defence*, 2022, https://www.eeas.europa.eu.

[9] See NATO, *Statement by the North Atlantic Council Concerning the Malicious Cyber Activities against Albania*, September 8, 2022; CCDCOE, *Homeland Justice Operations Against Albania*, 2022, https://cyberlaw.ccdcoe.org/wiki/Homeland_Justice_operations_against_Albania_(2022). Let it be permitted to refer to A.L. SCIACOVELLI, *Taking cyber-attacks seriously: the (likely) Albanian cyber aggression and the Iranian responsibility*, in *Osservatorio sulle attività delle organizzazioni internazionali e sovranazionali, universali e regionali, sui temi di interesse della politica estera italiana*, 2023, www.osorin.it.

[10] https://www.voanews.com/a/6734763.html; https://www.nato.int/cps/en/natohq/official_texts_207156.htm

[11] https://www.nato.int/cps/en/natohq/news_207552.htm?selectedLocale=en; https://www.nato.int/cps/en/natohq/official_texts_17120.htm.

This paper is structured as follows: it examines the most prominent types of cyberoperations below and above the use-of-force threshold of the prohibition of the use of force committed by states; it identifies the legal and technical challenges of their attribution to states, and it traces the possible solutions to the problem of international responsibility of states regarding the use of proxies to commit wrongful acts in cyberspace.

2. States often conduct illicit cyberoperations using their military and intelligence apparatus. However, in many cases, they prefer to use groups of professional criminal hackers, known as non-state actors. These include individuals, groups, or private security companies acting as *proxies* in executing hostile activities in cyberspace.

The UN Working Group on Mercenaries, in its 2021 report on cyber mercenaries, highlighted the increasing involvement of private actors in the cyber domain, such as cyber militias and Advanced Persistent Threat (APT) groups[12]. Cyber mercenaries are private actors engaged by states to conduct offensive or defensive cyberoperations to weaken or undermine the military capacities of adversary forces.

As outlined by the UN Open-Ended Intergovernmental Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination (OEIWG) in its Progress Report of 2024, one of the consequences of the use of cyber militias is the asymmetric nature of modern armed conflicts[13]. This has led to the proliferation of and military companies exacerbating conflicts dynamics and exposing the civilian population to the violation of human rights. These militias provide inherently covert opportunities to product, store, transfer, and deploy significant military capabilities with minimal organizational, financial and human resources compared to traditional industrial warfare. Recently, these

[12] See the *UN Working Group Report on the Use of Mercenaries as a Means of Violating Human Rights and Impeding the Exercise of the Right of Peoples to Self-Determination*, July 15, 2021, UN Doc. A/76/151.

[13] See Chair-Rapporteur of the UN Human Rights Council, *Progress Report on the fifth session of the Open-Ended Group Intergovernmental Working Group to Elaborate the Content of an International Regulatory Framework on the Regulation, Monitoring and Oversight of the Activities of the Private Military Companies* (*OEIWG Report 2024*), UN Doc. A/HCR/57/53.

APT have developed a cyber arsenal sometimes superior to the ones of the states[14].

Generally, non-state actors operating in cyber space are highly organized and have criminal affiliations in other states. They possess their own intelligence agencies, help desks and they purchase cheap cyber weapons kits and subscriptions to commit cybercrimes on digital platforms on behalf of their clients, such as states (crime-as-a-service).

Previously, these offensive capabilities were only available to states and this recent shift is partly due to the cheap commercial availability of cybercrime and ransomware tools, leading to the *privatization* of offensive cyber capabilities.

These criminal groups use sophisticated digital tools to exploit artificial intelligence[15]. This allows them to expand digital attack surfaces by exploiting the vulnerabilities of ICTs' systems and the weaknesses of human factors, i.e. using social engineering. Soon probably non-state actors will use post quantum computing to better prepare their malicious activities in cyberspace[16].

The goals pursued by criminal hackers are primarily economic and political. Economic motivations stem from the potentiality to realize huge profits from computer crimes, ranging from hundreds to millions of dollars, which allow for the self-financing of the criminal group. Political motivations are often linked to ideological choices (as with hacktivists and cyber terrorists) or to states' geopolitical strategies in the cyber arena. Examples include collectives online acting in international conflicts (e.g., Russia and Ukraine), in regional rivalries (e.g., India and Pakistan) and regional conflicts (e.g., Israel and Hamas, Israel and Palestine)[17].

---

[14] See *OEWG Report on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2021, Annex I, para. 19 (*OEWG Report 2021)*, par. 16; M. N. SCHMITT, S. WATTS, *Beyond State-Centrism: International Law and Non-State Actors in Cyberspace*, in *Journal of Conflicts&Security Law*, 2016, 595 ff; E. D. BORGHARD, S.W. LONERGAN, *Cyber Operations as Imperfect Tools of Escalation*, in *Strategic Studies Quarterly*, 2019, 122 ss.; J. BLESSING, *The Global Spread of Cyber Forces, 2000–2018*, 2021, https://ccdcoe.org.

[15] See *OEIWG Report 2024*, cit., 3.

[16] See *OEWG Report 2021*, cit., par. 16; R.J. BUCHAN, *Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm*, in *Journal of Conflict & Security Law*, 2016, 429 ff; K. MAČÁK, *Unblurring the Lines: Military Cyber Operations and International Law,* in *Journal of Cyber Policy*, 2021, 411 et seq.

[17] See M. BLAEZNER, *Hotspot Analysis: Regional Rivalry Between India-Pakistan: Tit-for-tat in Cyberspace*, Center for Security Studies, ETH Zurich, 2018; T. MIMRAN, *Israel-Hamas 2023 Symposium, Cyberspace, the Hidden Aspect of the Conflict*,

Despite their role as guarantors of international law within their boundaries, states often tolerate, sponsor, or even coordinate the activities of criminal hackers operating from the digital networks of their territories. Therefore, a significant challenge in international law is how to hold a sponsor state internationally responsible for the illegal conduct of non-state actors in cyberspace[18].

3. Hostile cyberoperations vary widely in nature, scale, and scope. The most prominent and frequent types include distributed denial of service (DDoS), ransomware, which can also be destructive, and cyber espionage[19]. The first two should be distinguished from cyber espionage, which usually serves informational and retaliatory tactics. Cyber espionage involves extracting information from networks without disrupting their functionality. It violates state's domestic laws, and generally does not violate international law, unless it is part of a complex and coordinated military operation[20].

---

https://lieber.westpoint.edu/cyberspace-hidden-aspect-conflict. On the nature of the conflicts between Israel and Hamas, and between Israel and Palestine, see A.A. KARIM, Press Statement of May 20, 2024, of the International Criminal Court Prosecutor. See K.C. KHAN, *Applications for Arrest Warrants in the Situation in the State of Palestine*, 2024, https://www.icc-cpi.int/news/statement-icc-prosecutor-karim-aa-khan-kc-applications-arrest-warrants-situation-state; J.B. QUIGLEY, *Karim Khan's Dubious Characterization of the Gaza Hostilities*, 2024, in https://www.ejiltalk.org.

[18] See V. M. BENATAR, *The Use of Cyber force: Need for Legal Justification?*, in *Goettingen Journal of International Law*, 2009, 378 ff; V. WOLTAG, J. CHRISTOPH, *Cyber Warfare*, in *Max Planck Encyclopedia of Public International Law*, Oxford, 2015, 7 ff; M. FINNEMORE, D. HOLLIS, *Beyond Naming and Shaming: Accusations and International Law in Cybersecurity*, in *The European Journal of International Law*, 2020, 970; F. DELERUE, *Cyber Operations and International Law*, Cambridge, 2020, 11-12.

[19] For a definition of cyber-attack, see M.N. SCHMITT, *Tallinn Manual 2.0*, cit., Rule 92, 415, a «cyber operation, whether offensive or defensive, […] is reasonably expected to cause injury or death to persons or damage or destruction of objects». The cited rule seems inspired by the notion of kinetic attack pursuant to Art. 49, par. 1, of the I Additional Protocol to the four Geneva Conventions of August 12, 1949, relating to the protection of victims of international armed conflicts, adopted in Geneva June 8, 1977, which states «[T]he expression "attacks" means acts of violence against the adversary, whether such acts are carried out for the purpose of offense or defense». M.N. SCHMITT, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, in *Columbia Journal of Transnational Law*, 1999, 885; M. ROSCINI, *Cyber*, cit., 10-18; J. BILLER, *The Strategic Use of Ransomware Operations*, in *International Law Studies*, 2023, 484.

[20] For O. A. HATHAWAY, R. CROOTOF, *The Law of Cyber-Attack*, in *California Law Review*, 2012, 829, cyber espionage is «the science of covertly capturing e-mail traffic, text messages, other electronic communications, and corporate data for the purpose of gathering national-security or commercial intelligence». On cyber espionage and international law see also M. N. SCHMITT, *Tallinn Manual 2.0*, cit., Rule 32, 168; R. BUCHAN, *Cyber Espionage and International Law*, Oxford-New York, 2019.

Specifically, cyberoperations are characterized by their multistage nature. Unlike conventional military or criminal acts, where effects are apparent shortly after the weapons are used, cyber weapons (such as logic bombs, worms, trojans, and malware etc.) can stay dormant for significant periods, can secretly alter data and can clandestinely compromise a network's operation. It often takes months to detect them and this ability to avoid detection distinguishes cyber from kinetic weapons and operations[21].

Other differences include the transnational nature of the cyber domain, which lacks physical borders, grants almost total anonymity to actors, and involves complex operations that are also often widespread and decentralized from a geographical point of view.

An example is the use of hundreds of thousands of botnets (zombies) by an actor (state or otherwise) to infect computers and Internet of Things (IoT) devices in another state, as seen in the operation against Estonia in 2007 conducted from the territories of many states and presumably backed by the Russian Federation[22].

Moreover, hostile digital activities are often carried out through the ICTs of multiple states, sometimes without their knowledge. This includes the state(s) of the launch of the operation, the state(s) whose ICTs are used for the malware transit, and the state(s) where the criminal offenses take place.

---

[21] See D.D. CLARK, S. LANDAU, *Untangling Attribution*, in *Harvard National Security Journal*, 2011, 531 and 533.

[22] A botnet is a network of computers infected with malicious software (malware) to be controlled remotely by a single actor - called bot master - to attack a target, without the real owners of the computers being aware of it, hence they are called zombies, thus increasing the resources and offensive capabilities at its disposal. Computers are forced to send spam, spread viruses, or launch DDoS attacks. In the case of Estonia, the attack was launched in conjunction with the Estonian Government's decision to remove the bronze statue of the unknown Soviet soldier from the main square of Tallinn, hence its attribution to the Russian Federation on the basis of elements collected by intelligence. These attacks led to the interruption of the functioning of the main ICT systems of public, financial and media bodies, causing an economic loss quantified between twenty-seven and forty million dollars. Specifically, the DDoS attack consists of sending a series of requests for information to an entity's information and communication system in order to block it. See R. SHACKELFORD, *An Introduction to the Law of Cyber War and Peace, in Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace*, Cambridge, 2014, 263; I. ZAHRA, I. HANDAYANI, D.W. CHRISTIANTI, *Cyber-attack in Estonia: A New Challenge in the Applicability of International Humanitarian Law*, in *Yustisia*, 2021, 48; D. BROEDERS, F. DE BUSSER, F. CRISTIANO, T. TROPINA, *Revisiting Past Cyber Operations In Light of New Cyber Norms and Interpretations of International Law: Inching Towards Lines in the Sand?*, in *Journal of Cyber Policy*, 2022, 108.

Currently, there is unanimous consensus among states about the applicability of international law to cyberspace, and first of the essential principle of the respect of state's sovereignty, whose application extends to the digital dimension as well[23]. However, differing positions have emerged among member states on whether it is necessary also to draft specific provisions for cyberoperations.

Specifically, the international legal framework for cyberspace was developed within the UN since the late 1990s. This international organization has been committed to promoting a shared vision among member states for an open, accessible, and peaceful digital ecosystem. The UN has also emphasized the safe and responsible use of ICTs, in accordance with international law and the UN Charter.

Starting in 2003, the UN Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security (hereinafter, GGE) and, subsequently, from 2019, the UN Open-Ended Working Group on Security of and in the Use of Information and Communication Technologies (hereinafter, OEWG) have produced a series of reports outlining the principles of international law applicable by consensus to cyberspace[24].

These reports are the principal reference for states on the application of international law, and specifically on international responsibility in cyberspace. They are the result of extensive diplomatic efforts and of the reflection of geopolitical tensions arising from the composition of the two UN working groups. The first group was established by the United States and the second one was the outcome of China and Russian Federation will. These groups are actively engaged in the elaboration of cyberspace principles that are enshrined, since 2015, in a decalogue of eleven voluntary non-binding

[23] See GEE, *Report on Developments in the Field of Information and Telecommunications in the Context of International Security*, July 22, 2015, UN Doc. A/70/174, 27 (*GEE Report 2015*); NATO, *Cyber Defence Pledge*, https://www.nato.int; Rapporteur of the Organization of American States, D.B. HOLLIS, *Improving Transparency – International Law and State Cyber Operations: Fourth Report*, OAS Doc. OEA/Ser.Q, CJI/doc 603/20 rev.1, 2020; UN General Assembly, *Program of Action to Advance Responsible State Behavior in the Use of Information and Communications Technologies in the Context of International Security*, res. of October 13, 2022, UN Doc. A/C.1/77/L.73.

[24] See UN General Assembly resolutions of 18 December 18, 2003 (UN Doc. A/RES/58/32), December 8, 2005 (UN Doc. A/RES/60/45), December 13, 2011 (UN Doc. A/RES/66/24), June 24, 2013 (UN Doc. A/68/98), January 9, 2014 (UN Doc. A/RES/68/243), December 30, 2015 (UN Doc. A/RES/70/237) January 2, 2019 (UN Doc. A/RES/73/266), July 14, 2021 (UN Doc. A/76/135), and October13, 2022 (UN Doc A/C.1/77/L.73).

norms of responsible state behavior in the use of Information and Communications Technologies (UN non-binding norms)[25].

This decalogue concerns with the maintenance of international peace and security in cyberspace in line with the principles of the UN Charter; the ban on using the state territory for internationally prohibited activities; the peaceful use of ICTs also in compliance with human rights; the respect for state sovereignty; the peaceful resolution of international disputes and the non-intervention in the internal and external affairs of a state through ICTs.

This decalogue enshrine obligations and principles of customary international law, particularly those embedded in the UN Charter, and it represents the essential, consolidated, cumulative, and evolving framework for conducts in the digital domain and to which reference will be made in this chapter[26]. As it will emerge in these pages and in the following chapters of this book, the specific contents and the practical application of the obligations and principle contained in the decalogue are still under evolution and evaluation particularly because of their recent articulation about the state's international responsibility in cyberspace.

Specifically, upon closer examination, it is evident that this framework lacks specific guidelines regarding illicit digital operations that may fall under the prohibition in Article 2, Paragraph 4 of the UN Charter. This norm prohibits the threat and use of armed force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the UN[27]. Furthermore, it does not address the exercise of the right of self-defense in response to a cyber-attack.

From a legal perspective, depending on the extent of their intrusion or on their effects, cyberoperations may violate the principles of state's sovereignty, of non-intervention or even the of the prohibition of the threat or use of force in international relations.

---

[25] GEE, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 22 July, 2015, UN Doc. A/70/150, 12; OEWG, *Report on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2021, UN Doc. 75/816; *Ibidem*, *Report of the on Security of and in the Use of Information and Communications Technologies 2021–2025*, August 8, 2022, UN Doc. A/77/275 (*Report 2022*). See also in this book, GARGIULO, *The United Nations and Cybersecurity*, cit.

[26] See *Report OEWG 2022*, cit., par. 15 f., 10 f.

[27] See M.N. SCHMITT, *Classification of Cyber Conflict*, in *Journal of Conflict & Security Law*, 2012, 251.

Therefore, cyberoperations mainly may be categorized in operations i) that are *above* and ii) that fall *below* the use-of-force threshold enshrined in Article 2, Paragraph 4 of the UN Charter[28]. The choice of this categorization is due to the different legal consequences whether the cyberoperation falls in one of the two categories.

Starting from the type of cyberoperations whose effects are *below* the use-of-force threshold (and dealing with the 'above threshold' operations in the next paragraph), they might constitute a violation of the principle of territorial sovereignty (as it extends to the ICTs infrastructures located within its territory) and of other international norms and principles that flow from it[29].

Unauthorized intrusion of the ICTs of a State itself constitutes a violation of its territorial sovereignty along with accessing to i) to steal, manipulate, or destroy data that resides in the target information systems, and ii) to disrupt the ICTs functions. As suggested by the arbitration ruling on the *Island of Palmas* (1928), territorial sovereignty involves a state's exclusive right to exercise power over a specific area[30].

---

[28] See M.C. WAXMAN, *Cyber Attacks as "Force" Under UN Charter Article 2(4)*, in *International Law Studies*, 2011, 43; S. WATTS, *Low-Intensity Cyber Operations and the Principle of Non-Intervention*, in J.D. OHLIN, K. GOVERN (eds), *Cyber War and Ethics for Virtual Conflicts*, Oxford, 2015; M. ROSCINI, *International Law and the Principle of Non-Intervention: History, Theory, and Interactions with Other Principles*, Oxford, 2024, 374 ff.

[29] According to Rule 1 of the *Tallinn Manual 2.0*, cit., «[t]he principle of State sovereignty applies in cyberspace». GEE *Report 2015*, paras. 27-28. According to M.N. SCHMITT, *Tallin Manual 2.0,* cit., Rule 4, 12 ff, «[C]yber operations that prevent or disregard another State's exercise of its sovereign prerogatives constitute a violation of such sovereignty and are prohibited by international law» on the assumption that «States enjoy sovereignty over cyber infrastructure, persons, and cyber activities located on their territory. This includes both public and private cyber infrastructure». The 'sub-threshold' operations might also represent the instrument of a military strategy: the hybrid warfare. Hybrid warfare is based above all on the use of unconventional tools, such as IT and disinformation campaigns, interference in electoral processes and the exploitation of irregular migratory flows, to name a few examples. It is an offensive strategy whose objective is to undermine the national security of a country. On this topic see M.N. SCHMITT, S. WATTS, *Beyond State-Centrism*, cit., 600; F.G. HOFFMAN, *Conflict in the 21st Century: The Rise of Hybrid Wars*, 2007, www.potomacinstitute.org; M. CLARK, *Russian Hybrid Warfare*, 2020, https://www.understandingwar.org; G. Simons, Y. DANYKM, T. MALIARCHUK, *Hybrid War And Cyber-Attacks: Creating Legal and Operational Dilemmas, Global Change*, in *Peace & Security*, 2020, 337 ff; NATO, *NATO's Response to Hybrid Threats*, 2021, www.nato.int; on the notion of cyber intervention see I. KILOVATY, *The International Law of Cyber Intervention*, in N. TSAGOURIAS, R. BUCHAN (eds.), *Research Handbook*, cit., 99 ff.

[30] Permanent Court of Arbitration, *Island of Palmas* (The Netherlands v. United States of America), arbitration award April 4, 1928, 838-839; see Rule 4 of *Tallin Manual 2.0,* cit., on "Violation of sovereignty" states «[A] State must not conduct cyber operations that violate the sovereignty of another State», 17.

For instance, a cyberoperation that affects the confidentiality, integrity, or availability of data or disrupts the functioning of computer systems and produces physical effects constitutes such a violation, such as impacting critical infrastructures (e.g., power utilities, water supplies), causing widespread effects (e.g., power outages), or interfering with the functioning of public or private healthcare facilities (e.g., hospitals).

It is noteworthy to distinguish between two approaches to find a violation of sovereignty: the *de minimis* approach, that requires a sufficient degree of infringement of the target state's territorial integrity that might be caused by the disruption of ICTs, or by an interference with/or by the usurpation of its inherently governmental functions and the presence of physical damages, and the penetration-based approach, that argues that every penetration of computer networks within a state's territory violates its sovereignty[31].

Moreover, a cyberoperation attributable to a state may constitute a violation of the *principle of non-intervention* in internal affairs of a state when it involves an act of coercion within its domestic jurisdiction, potentially constituting an internationally wrongful act.

The principle of non-intervention is clearly stated in some UN General Assembly declarations[32], and in the light of the international Court of Justice (ICJ) jurisprudence the violation of this principle can occur when two conditions are met cumulatively: the action constitutes a coercive interference into the domestic jurisdiction[33].

---

[31] Few states adhere to the latter approach, for instance according to the Ministry of Defence of France, *International Law Applied to Operations in Cyberspace*, 2019, «any cyber-attack against French digital systems or any effects produced on French territory by digital means by a State organ [or otherwise attributable to a State] constitutes a breach of sovereignty», https://cyberlaw.ccdcoe.org/wiki/National_position_of_France_(2019)#Due_diligence. For the *de minimis* approach see Rule 4, *Tallinn Manual 2.0*, cit., 20.

[32] See the Principles III and VI of the UN General Assembly Declaration on Principle of International Law Concerning Friendly Relations and Cooperation among States in Accordance with the UN Charter UN Doc. A/Res/2526(XXV), of October 24, 1970, UN Doc. A/Res/2526; the Declaration on the enhancement of the effectiveness *of the* principle of refraining from the threat or use of force in international relations, of November 18, 1987, UN Doc. A/Res/42/22; the Principles I and VI of the Final Act of the Helsinki Conference on Security and Cooperation in Europe, August 1, 1975. See M. ROSCINI, *International Law and the Principle of Non-Intervention: History, Theory, and Interactions with Other Principles*, Oxford, 2024, 374 ff.

[33] See International Court of Justice, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua* v. *United States of America) (Nicaragua case), Merits,* Judgment June 27, 1986, in *ICJ Reports*, 1986, 98 ff, paras. 187 ff, 106, para. 202; Id., case *Armed Activities on the Territory of the Congo* (*Democratic Republic* of the *Congo v. Uganda*), Judgment

Starting with the first criterion, coercion can involve forcing another state to do or refrain from doing something under threat of specific, serious, and credible harm, or taking control of a certain situation and forcibly imposing a certain action.

The second criterion involves the domestic jurisdiction, which consists of coercion of the target state in matters where it has no obligations under international law, either customary or conventional. Examples include «the choice of a political, economic, social and cultural system, and the formulation of foreign policy»[34].

In cyberspace questions remain about which affairs fall into the domestic jurisdiction of a state, and how to define the element of coercion. It may be the case of cyberoperations which disrupt the capacity of a state to conduct an electoral process, or which alter its results through manipulation of electronic voting infrastructures.

Corollary of the principle of state sovereignty is the *due diligence* principle under which every state is under an obligation «not to allow knowingly its territory to be used for acts contrary to the rights of other States», in accordance with the ICJ *Corfu Channel* case (1949)[35]. The *due diligence* principle is enshrined in Norm C of the UN non-binding norms that emphasizes that states should not knowingly permit their territory to be used for wrongful acts via ICTs[36].

Furthermore, under Norm F of the cited UN non-binding norms states should also «not conduct or knowingly support ICT activity

---

December 19, 2005, in *ICJ Reports*, 2005, 164. See also Rule 66 of the *Tallinn Manual 2.0*, cit., which states: «[A] State may not intervene, including by cyber means, in the internal or external affairs of another State», 312.

[34] ICJ, *Nicaragua* case, cit., para. 202.

[35] ICJ, The *Corfu Channel Case* (*United Kingdom* v. *Albania*), Judgment of April 9, 1949, ICJ Reports, 22; Id., Case *Pulp Mills on the River Uruguay* (*Argentina* v. *Uruguay*), Judgment of April 20, 2010, *ICJ Reports*, 2010, para. 101.

[36] See GEE *Report of 2015*, para. 13 (c); N.M. SCHMITT, *In Defense of Due Diligence in Cyberspace*, in *Yale Law Journal Forum*, 2015, 68; Rule 6, *Tallinn Manual 2.0*, cit., 30, that reads as follows: «[A] State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States». On this subject see C. BANNELIER-CHRISTAKIS, *Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?*, in *Baltic Yearbook of International Law*, 2014, 23, 37; K. KITTICHAISAREE, *Public International Law of Cyberspace*, cit., 33; I. COUZIGOU, *Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations*, 2018, 37, https://aura.abdn.ac.uk; A. COCO, T. DE SOUZA DIAS, "*Cyber Due Diligence": A Patchwork of Protective Obligations in International Law*, in *European Journal of International Law*, 2021, 771; ID., *Cyber Due Diligence in International Law*, Oxford, 2022, 47.

contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public» of other states[37].

This means that a state is obliged to prevent harmful cyber activities, that reaches the requisite threshold of harm[38], and that are originating from, passing through, or occurring in any area under its exclusive control (e.g. for the misuse of its ICTs) when it knows - or should have known - about such activities, especially when they infringe on the rights of another state. Knowledge can be determined by the notification by the victim-state that has identified the state or states from the territories of which the malicious cyber transmissions occur. Therefore, the notified state is expected to take reasonable, proportionate, and effective measures to prevent, halt, respond, and address the harmful transboundary cyberoperations that can be committed by its organs or by non-state, even if the identity of the hostile operation's initiator is unknown[39]. The latter notion should include unregulated (national or international) security companies that should be held accountable for their activities in cyberspace to avoid impunity for their actions[40]. Thus, a state may be responsible for harmful international for its failure to prevent illicit cyberoperations. However, it is not expected that the state should monitor all the ICTs activities within its territory, as it is an 'expectation of means', but it should respect the duty of prevention and vigilance[41].

4. The cyberoperations whose effects are *above* the use-of-force threshold are one of the most complex issues in international cyber law.

---

[37] Norm F of the UN non-binding norms. See R.J. BUCHAN, *Cyberspace, Non-State Actors*, cit., 451 ff.

[38] ICJ, Case *Pulp Mills on the River Uruguay*, cit., parr. 30-34.

[39] See the UN International Law Commission Draft Articles on the Prevention of Trans–Boundary Harm from Hazardous Activities that states that the standard of due diligence to assess the conduct of a state would be that which would be deemed «appropriate and proportional to the degree of risk of trans-boundary harm in the particular instance» (2001) A/56/10, 154.

[40] Also noteworthy is the OEWG Working paper, Multiple states' views on best practices relating to the implementation of norm 13(c), 2024, 2, which clarifies context and content of the *due diligence* principle, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/OEWG_Working_paper_-_Best_practices_relating_to_the_implementation_of_norm_13(c).pdf.

[41] See GGE, Report of the 2019-2021, UN Doc. A/76/135, par. 30 a.

As anticipated, this prohibition is regulated in Art. 2, para. 4 of the UN Charter and in numerous Declarations of principles of the UN General Assembly. They define the interpretative and applicative contours of the prohibition of the use of force, and the threat of the use of force, in international relations[42]. Initially, the ban was recognized as a norm of conventional international law, but subsequently the ICJ recognized its nature as both a customary norm and as a *jus cogens* norm[43]. The only agreed exception to the prohibition in question is the individual and the collective legitimate defense, which is regulated by Art. 51 of the UN Charter[44].

Specifically, the use of armed force implies a violation of Art. 2, para. 4 of the UN Charter if it reaches a certain threshold in terms of extent, duration and physical destruction, as stated by the ICJ. The Court distinguished the most serious forms of use of force - qualified as an armed attack - from the less serious forms, qualified as a mere use of force, such as border clashes/incidents[45]. The Ethiopia-Eritrea Complaints Commission reached a similar assessment in its decision (2005), in which it stated that minor border incidents, while constituting a violation of the rules relating to the prohibition of the use of force, are not comparable to an armed attack and, therefore, do not give the right to react in self-defense[46].

---

[42] On this topic see the contributions of V. STARACE, *Uso della nell'ordinamento internazionale*, in *Enciclopedia Giuridica*, vol. XXXII, Roma, 1994, 1 ff; B. SIMMA (ed.), *The Charter of the United Nations, A Commentary*, 2° ed., vol. 1, Oxford, 2002, 794; A. CASSESE, *International Law*, Oxford, 2005, 56; P. GARGIULO, *Uso della forza (Diritto internazionale)*, in *Enciclopedia del Diritto*, *Annali*, vol. V, Milano, 2012, 1376-1430; A. LANCIOTTI, A. TANZI, *Uso della Forza e legittima difesa nel diritto internazionale contemporaneo*, Napoli, 2012; O. GÖRR, *Use of Force, Prohibition of*, in *Max Planck Encyclopedia of Public International Law*, Oxford, 2019, 1; B. CONFORTI, M. IOVANE, *Diritto internazionale*, Napoli, 2022, 209; E. CANNIZZARO, *Diritto internazionale*, Torino, 2022, 21; U. VILLANI, *Lezioni di diritto internazionale*, Bari, 2023, 243.

[43] *Nicaragua* case, cit., parr. 65, 99 s., 109, 115 e 190. See M.N. SCHMITT, M. WELLER, (eds.), *The Use of Cyber Force and International Law, The Oxford Handbook of the Use of Force in International Law*, Oxford, 2015, 1110; D. AKANDE, A. COCO, T. DE SOUZA DIAS, *Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies*, in *International Law Studies*, 2022, 4.

[44] V. M. HOISINGTON, *Cyberwarfare and The Use of Force Giving Rise to The Right of Self-Defense*, in *Boston College International and Comparative Law Review*, 2009, 439-440; O. KESSLER, W. WERNER, *Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare*, in *Leiden Journal of International Law*, 2013, 807.

[45] ICJ, *Nicaragua* case, cit., 101, para. 191.

[46] See Eritrea Ethiopia Claims Commission, Partial Award, *Jus ad Bellum*, Ethiopia's Claims 1-8, December 19, 2005, para. 11; see N. RONZITTI, *Diritto internazionale dei conflitti armati*, 6° ed., Torino, 2017, 37.

Specifically, given the *sui generis* nature of the digital domain regarding the maintenance of international peace and security, it is necessary to verify the outcome of the application of the existing obligations of international law, that have been shaped for the physical world. The issue primarily concerns the qualification of a transnational malicious cyberoperation as an "armed attack", considering that, according to the ICJ, only the most severe forms of force, in terms of intensity and gravity, and physical destruction can be classified as such[47].

In the absence of an official definition of a cyber-attack in international law, the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (hereinafter, Tallinn Manual 2.0) provides useful guidance. In digital space, crossing the threshold of the use of force depends not on the target of the attack (the target-based approach), nor on the digital means employed, that are digital codes (the weapons-based approach), but rather on the effects of the cyberoperation from a *quantitative* and *qualitative* perspective (the so-called *effects-based approach,* Rule 92).

In the *quantitative* approach, the *Manual* (Rule 69) suggests that a cyberoperation constitutes a violation of the prohibition on the use of force if its *scope* and *effects* are comparable to those of a "above threshold" kinetic operation[48]. Additionally, about the weapon used, in the ICJ advisory opinion on the *Lawfulness of the Threat or Use of Nuclear Weapons* (1996), the prohibition on the use of force is regardless of the type of weapons used, since this prohibition refers to any type of force, even immaterial[49].

Regarding the *qualitative* approach, the *Tallinn Manual 2.0* specifies that for a malicious cyberoperation to be considered an armed attack, damage to tangible and intangible assets (including digital data) must be such - or may reasonably likely be as such - that

---

[47] On this topic see Y. DINSTEIN, *Computer Network Attacks and Self-Defense*, in M.N. SCHMITT, B.T. O'DONNELL (eds.), *Computer Network Attack and International Law*, 2002, 38, https://digital-commons.usnwc.edu; D.B. SILVER, *Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter*, in *International Law Studies Series US Naval War College*, 2002, 73; M. ROSCINI, *Cyber operations as a use of force*, in N. TSAGOURIAS, R. BUCHAN (eds.), *Research Handbook*, cit., 301 ff.

[48] See ICJ, case *Oil Platforms*, (*Islamic Republic of Iran* v. *United States of America*), Judgment of November 6, 2003, *ICJ Reports*, 2003, par. 51 and 72, which does not exclude the possibility that even a single attack (such as one against a warship), could justify the exercise of the right to self-defense.

[49] See S. LA PISCOPÌA, *Necessità di una definizione delle armi cibernetiche*, in *Eurasia*, 2022, 37, and in this book, ID., *The Regulatory Relevance*, cit.

it alters their normal use and functioning that could lead to the death and wounding of people or the destruction of property. An example would be tampering with the ICT systems of critical infrastructures, particularly in the operational technology (OT) sector, such as dams, electrical grids, or nuclear power plants. Malfunctions or tampering in these areas could cause widespread destruction or fires, resulting in physical effects—both direct and indirect—on the civilian population and the security of a state. To this end, it is advisable that the requirement of *kinetic equivalence* is respected, that is if a malicious operation causes – or is reasonably likely to cause - deaths, injuries, and significant material damages comparable to those normally resulting from an kinetic armed attack. For example, consider tampering with the IT systems of a dam downstream of a densely populated area, which results in the dam's opening and subsequently leads to the destruction of the inhabited areas and the death of the residents.

The first instance of this type of operation occurred following the *Stuxnet* attack in 2010, which was likely carried out with the aim of disrupting Iran's nuclear program. In this case, the introduction of a virus called Stuxnet into the computer system of the Natanz nuclear power plant in Iran caused the 1,000 cooling turbines of the plant to malfunction, leading to the shutdown of the facility[50]. This event highlights the *potential* consequences in the physical world if the cyber sabotage had not been limited to merely disabling the turbines, but instead had been aimed at causing an explosion at the nuclear power plant.

5. Once the cyberoperation has been qualified as a violation of a norm of international law, it should be attributed to a state eventually to declare its international responsibility. The activity of determining the responsibility for a cyber activity or operation to a state - called

[50] For Y. DINSTEIN, *War, Aggression and Self-Defence*, 5° ed., Cambridge, 2011, 105, «[T]he most egregious case is the wanton instigation of a core-meltdown of a reactor in a nuclear power plant, leading to the release of radioactive materials that can result in countless casualties if the neighboring areas are densely populated. In all these cases, the Computer Network Attack would be deemed an armed attack». See D.B. HOLLIS, *Could Deploying Stuxnet Be a War Crime?*, in *OpinioJuris.org*, 2011; S. HAATAJA, N. SAMULI, A. AKHTAR-KHAVARI, *Stuxnet and International Law on the Use of Force: an Informational Approach*, in *Cambridge International Law Journal*, 2018, 79; P. SINGER, *Stuxnet and Its Hidden Lessons on The Ethics of Cyberweapons*, in *Case Western Reserve Journal of International Law*, 2015, 132.

attribution - is a complex procedure due to the near-complete anonymity provided by cyberspace and other technical issues, especially when the cyberoperation has been committed by non-state actors. Attribution is a state's prerogative and involves establishing the connection between an agent's conduct (action or omission) and a state. This process involves three distinct sub-procedures: the technical sub-procedure, the legal and the political one.

The challenges of technical attribution in cyber activities revolve around identifying technical indicators and collecting the evidence that are needed to attribute cyber conduct to a state.

The *technical sub-procedure* involves a factual investigation aimed at identifying, with a certain degree of certainty, the source and the author of a cyberoperation, the associated network infrastructure, and the cyber tools used. It is based on a scientific examination of the digital and factual evidence of the conduct.

The identification of the source or the computer(s) used by the criminal hacker is possible identifying its Internet Protocol (IP) that gives also its location, while it is very difficult to identify the person operating it. This may be established thanks to confidential information disclosed by the intelligence agencies that may act alone or in cooperation with cyber security companies. It is well known that criminal hackers use sophisticated techniques to erase identifying evidence (fingerprints), and to obscure the source of the attack, and they orchestrate additional attack phases at different times and from various network infrastructures across multiple states[51]. For example, they anonymize their IP addresses using The Onion Router (Tor) and Virtual Private Networks (VPNs), and they encrypt their communications using servers, that can be located in a third country[52].

[51] See The NATO Cooperative Cyber Defence Centre of Excellence, *Mitigating Risks Arising from False-Flag and No-Flag Cyber Attacks*, https://ccdcoe.org, that states «[I]t is not enough to just locate a source IP address (unless looking solely at active defence): the identity of the attackers must be determined, as well as the parties they were acting on behalf of must also be unmasked». R. Cohen, *Cyberspace as/and Space*, in *Columbia Law Review*, 2007, 210 ff.; E. JENSEN, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, in *Stanford Journal of International Law*, 2002, 207; E.D. GRAHAM, *Cyber Threats and the Law of War*, in *Journal of National Security Law and Policy*, 2010, 89; H. PIHELGAS, *Back-Tracing and Anonymity in Cyberspace*, K. ZIOLKOWSKI (ed.), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, NATO CCDCOE Publication, Tallinn, 2013, 31, https://ccdcoe.org; N. TSAGOURIAS, *The Legal Status of Cyberspace*, N. TSAGOURIAS, R. BUCHAN (eds), *Research Handbook*, cit., 13 ff.

[52] See S. KANUCK, *Sovereign Discourse on Cyber Conflict Under International Law*, in *Texas Law Review*, 2010, 1573–5; D.D. CLARK, S. LANDAU, *Untangling Attribution*, cit., 530;

Another example is when malicious cyberoperations are conducted by one or more bot-masters who infiltrate network infrastructures in different states to coordinate simultaneous malicious activities against a target state using botnets (employing IT systems owned by third parties). In such cases, it is extremely challenging to trace the bot-master, especially when actions cross multiple jurisdictions[53].

Additionally, malicious cyberoperations can be intentionally falsely attributed by criminal hackers to an APT (that usually is state sponsored) through the spoofing techniques, for instance using malware codes that have been previously employed by the APT thus creating a *false flag* operation. Such operations pose the risk of prompting the victim state to react against an innocent third state.

Once the perpetrator has been identified based on the available digital evidence, the *legal sub-procedure* establishes the degree of the international responsibility of the state that has directed, orchestrated or sponsored the cyberoperations.

In this context, it might arise the issue of the lack of sufficient evidence due to the *sui generis* nature of cyberspace.

According to the UN General Assembly, the indication that a cyber illicit activity can be traced back to or originates from the territory of a state (or its network infrastructures), or that the codes appear traceable to that state, may not constitute sufficient evidence to attribute the operation to the state[54]. For the ICJ «claims against a State involving charges of exceptional gravity must be proven by

---

J.S. DAVIS II, *Stateless Attribution: Toward International Accountability in Cyberspace*, in *UCLA Law Review,* 2017, 9, www.rand.org; C. PAYNE, L. FINLAY, *Addressing Obstacles to Cyber-Attribution: A Model Based on State Response to Cyber-Attack*, in *George Washington International Law Review*, 2017, 49 ff.

[53] See P. ROGUSKI, *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views*, in *Policy Brief, The Hague Program for Cyber Norms*, 2020, https://www.thehaguecybernorms.nl.

[54] UN General Assembly, Resolution on the *Developments in the Field of Information and Telecommunications in the Context of International Security*, December 11, 2018, UN Doc. A/RES/73/27, par. 1.2. See *Tallinn Manual 2.0*, cit., 82 and 91; M.J. SKLEROV, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, in *Military Law Review*, 2009, 12, that affirms the objective State's responsibility; W. HEINTSCHEL VON HEINEGG, *Territorial Sovereignty and Neutrality in Cyberspace*, in *International Law Studies*, 2013, 123; M. ROSCINI, *Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations*, in *Texas International Law Journal*, 2015, 233 ff; M. FINNEMORE, D.B. HOLLIS, *Beyond Naming and Shaming*, cit., 571 ff.

evidence that is fully conclusive»[55]. Although in some cases an additional problem might arise due to the lack by developing states of the necessary technological resources and expertise to conduct the technical attribution process effectively.

A solution has been proposed by the GEE that encourages states to facilitate the tracing of hostile activities on critical information infrastructures and, when appropriate, disclose this information to other states. In case of an ICT incident, the affected state should notify the state from which the hostile activity is emanating, although the receiving of the notification does not imply the acknowledgment of the responsibility on the receiving state[56].

At the conclusion of these two sub-procedures, the state decides whether to declare (publicly or otherwise) the responsibility of the state actor for the sponsorship or direction of the cyberoperation (the political *sub-procedure*)[57].

6. In international law attribution is «the operation of attaching a given act or omission to a State» and to this end it is worth mentioning the Draft Articles on the Responsibility of States for Internationally Wrongful Acts of 2001 (herein after ARSIWA), developed by the UN International Law Commission, that relies on the relationship between individuals with a particular state[58]. In this regard, the ARSIWA's

[55] ICJ, case *Application of the Convention on the Prevention and Punishment of the Crime of Genocide*, (*Bosnia and Herzegovina* v. *Serbia and Montenegro*), Judgment February 26, 2007, *ICJ Reports*, 2007, parra. 43, 208 and 90; case *Oil Platforms*, cit., parr. 161, 189 e 190, and see the separated opinion of Judge R. Higgins that states that «the more grave the charge the more confidence there must be in the evidence», parra. 30-39. See the states' positions in GEE, *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 Behavior in Cyberspace in the Context of International Security Established Pursuant to General Assembly Resolution* 73/266, July 13, 2021, 84, UN Doc. A/ 76/136. See A. GHAPPOUR, *Tallinn, Hacking, and Customary International Law*, in *American Journal of International Law Unbound*, 2017, 224; J.N. MADUBUIKE-EKWE, *Cyberattack and the Use of Force in International Law*, in *Beijing Law Review,* 2021, 223 ff.

[56] See OEWG *Report 2021*, cit., para. 71 (g).

[57] See E.M. MUDRINICH, *Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem*, in *Air Force Law Review*, 2012, 167; K. EICHENSEHR, *The Law & Politics of Cyberattack Attribution*, in *University of California Los Angeles Law Review*, 2020, 67; N. TSAGOURIAS, M.D. FARRELL, *Cyber Attribution: Technical and Legal Approaches and Challenges*, in *European Journal of International Law*, 2020, 941.

[58] See *Draft Articles on the Responsibility of States for Internationally Wrongful Acts*, in *Yearbook of the International Law Commission*, 2001, vol. II, Part 2, 26 ff and 47 f. See C. ANTONOPOULOS, *State Responsibility in Cyberspace*, in N. TSAGOURIAS, R. BUCHAN (eds.),

rules might be applied to malicious operations carried out in cyberspace, given the customary nature of most of them, although with certain difficulties.

To satisfy the evidentiary requirements for the attribution procedure it is fundamental to identify the link between the non-state actors that conducted the cyberoperation and the state that has organized, sponsored, or coordinated them. As already said, states are *outsourcing* military activities in cyberspace to avoid direct responsibility for violating the prohibitions of international law, like the practices seen in the sponsorship of international terrorism.

In the ARSIWA it is affirmed that the international responsibility of a state arises when the international offense is committed by its officials or, in specific cases, by private citizens. Specifically, Article 4 of the ARSIWA addresses conduct carried out by state bodies in an official capacity as *de jure* state organs[59]. For example, this includes malicious cyberoperations conducted by the National Cyber Security Center or by intelligence and military combat units organized[60].

According to Article 5 of the ARSIWA, the international responsibility of a state can also be asserted if persons or entities exercise governmental functions act on its behalf [61].

Additionally, under Article 11 of the ARSIWA, a state is internationally responsible for acts carried out by non-state actors if it recognizes these acts as its own, as confirmed by the ICJ's jurisprudence[62], and, *ex* Article 8 of the ARSIWA, a state is

---

Research Handbook, cit., 113 ff; A. STIANO, *Attacchi informatici e responsabilità internazionale dello Stato*, Napoli, 2023, 119 ff.

[59] See Art. 4, para. 1, of the ARSIWA, cit., named "Conduct of organs of a State", reads: «[T]he conduct of any State organ shall be considered an act of that State under international law, whether the organ exercises legislative, executive, judicial or any other functions, whatever position it holds in the organization of the State, and whatever its character as an organ of the central Government or of a territorial unit of the State». See Rule 15 of the *Tallinn Manual 2.0*, cit.

[60] See U.S. Congressional Research Service, *Russian Cyber-Units*, 2022, https://crsreports.congress.gov.

[61] Under Art. 5 of the ARSIWA, cit., named "Conduct of persons or entities exercising elements of governmental authority", «[T]he conduct of a person or entity which is not an organ of the State under article 4 but which is empowered by the law of that State to exercise elements of the governmental authority shall be considered an act of the State under international law, provided the person or entity is acting in that capacity in the particular instance»; see Rule 15, *Tallinn Manual 2.0*, cit.

[62] According to Art. 11 of the ARSIWA, cit., "Conduct acknowledged and adopted by a State as its own", states that: «[C]onduct which is not attributable to a State under the preceding articles shall nevertheless be considered an act of that State under international law if and to the extent that the State acknowledges and adopts the conduct in question as its

responsible if it provides non-state actors with instructions for carrying out operations, or if it directs or controls them. In this case, non-state actors or entities are 'elevated' to *de facto* state agents or organs[63].

For the ICJ the *de facto* states organs can be identified as «persons, groups of persons or entities [that], may for purposes of international responsibility, be equated with state organs even if that status does not follow from internal law», if they «act in 'complete dependence' on the respondent State of which they are ultimately the instrument». It means that a state must exercise effective control through instructions over each individual operation and throughout the entire duration of the operation (the "effective control" test)[64].

This might establish a scenario of 'indirect' aggression, as outlined in the UN General Assembly's resolution on the definition of aggression (Resolution 3314(XXIX))[65].

---

own». Regarding the case of the *United States Diplomatic and Consular Staff in Tehran*, (*United States of America* v. *Islamic Republic of Iran*), judgment of May 24, 1980, *CIJ Reports*, 1980, Ayatollah Khomeini had approved the occupation of the American embassy and consulate premises and the taking of the staff hostages by Islamic students among the 1979 and 1981. Thus, according to the ICJ, in this case, «[T]he approval given to these facts by the Ayatollah Khomeini and other organs of the Iranian State, and the decision to perpetuate them, translated continuing occupation of the Embassy and detention of the hostages into acts of that State. The militants, authors of the invasion and jailers of the hostages, had now become agents of the Iranian State for whose acts the State itself was internationally responsible», par. 74.

[63] Art. 8 of the ARSIWA, named "Conduct directed or controlled by a State", affirms: «[T]he conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct». See Rule 17, a), of the *Tallinn Manual 2.0*, cit.; M.N. SCHMITT, L. VIHUL, *Proxy Wars in Cyber Space: The Evolving International Law of Attribution*, in *Fletcher Security Review*, 2014, 53; K. MAČÁK, *Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors*, in *Journal of Conflict and Security Law*, 2016, 405; W. BANKS, *State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0*, in *Texas Law Review*, 2017, 1487 ss.

[64] ICJ, *Nicaragua* case, cit., parr. 64 f, 106, 109, 112, 115, and the case on *Application of the Convention on the Prevention and Punishment of the Crime of Genocide*, cit., parr. 201, 205, 211-215, 396, and 400-407. For M.N. SCHMITT, *Tallinn Manual 2.0*, cit., 328, "[T]he Court sees no reason to deny that, in customary law, the prohibition of armed attacks may apply to the sending by a State of armed bands to the territory of another State, if such an operation, because of its scale and effects, would have been classified as an armed attack rather than as a mere frontier incident had it been carried out by regular armed forces Nicaragua", 93 par. 195. See also L. BLANK, *International Law and Cyber Threats from Non-State Actors*, in *Israel Yearbook on Human Rights*, 2013, 111.

[65] See UN General Assembly, Resolution on the definition of aggression (Resolution 3314(XXIX)) adopted by *consensus* on December 14, 1974, Art. 3. On this topic see C. KRESS, *Gewaltverbot und Selbstverteidigungsrecht nach der Satzung der Vereinten Nationen*

On this topic a different approach was taken by the Appeals Chamber of the UN *ad hoc* International Criminal Tribunal for crimes committed in former Yugoslavia in the *Tadić* case (1999). The Tribunal held that acts carried out by a military or paramilitary group could be considered acts of *de facto* organs of the state, thereby implicating the state's responsibility, if the group is under the overall control of the state. This approach (known as the "overall control" test) applies beyond «the mere financing or equipping […] and involv[es] also participation in the planning and supervision of military operations»[66].

It should be noted that these two approaches to legal attribution (the effective control and the overall one) are both challenging to be satisfied due to the technical difficulties in demonstrating the factual connection between the state and criminal hackers. As a matter of fact, a cyberoperation rarely can be reliably attributed, as it often can be only geolocated. Specifically, it is difficult to demonstrate a state's effective control over the hacker groups if it is based on factors such as the provision of weapons, training, intelligence sharing, target selection, operational, logistic and financial support, and the guarantee of a safe haven in the state's territory[67]. All these requirements for evidence are difficult to prove due to the intangible nature of ICT tools, to the virtual nature of training, to the encrypted communications, and to the use of cryptocurrencies to provide economic support, which are often untraceable, just to cite a few.

---

bei staatlicher Verwicklung in Gewaltakte Privater, Berlin, 1995, 314–19, who supports the existence of a *lex specialis* on attribution based on the 'substantial involvement-limb' in Art. 3(g) of the 1974 Definition of Aggression.

[66] See International Criminal Tribunal *ad hoc* for crimes committed in the Former Yugoslavia, Appeals Chamber, *Prosecutor* v. *Tadić*, Case No IT-94-1-A, Judgment July 15, 1999, 118-122, 131, 137, 145, and 154. In this case the Appeals Chamber found that Serbia had supported and coordinated the general planning of the military activity of the Bosnian Serb paramilitary troops materially and with funding. For the Appeals Chamber a state «wields overall control over the group, not only by equipping and financing the group, but also by coordinating or helping in the general planning of its military activity». In this case, «it is not necessary that, in addition, the State should also issue, either to the head or to members of the group, instructions for the commission of specific acts contrary to international law», par. 131. See Y. DINSTEIN, *War, Aggression*, cit., 104.

[67] UN General Assembly, January 22, 2001, invites member states to «eliminate safe havens for cybercriminals», par. 1(a), U.N. Doc. A/RES/55/63, and ICJ, *Nicaragua* case, cit., parr. 95-97, 99, 104, 106, 109, 112, 115. W. BANKS, *State Responsibility*, cit., 1490. On the notions of effective, general and indirect control operated by the State on *de facto* agents and which has emerged in international law and jurisprudence, see J. KURBALIJA, *State Responsibility in Digital Space*, in *Swiss Review of International and European Law*, 2016, 15.

Additionally, there is often a lack of will on the part of states to control the activities of online criminal groups. This reluctance is due to outsourcing of the commission of malicious cyberoperations that partly occurs because states lack the necessary technological tools, expertise, or the capability to keep pace with the rapid developments in information technology.

According to the UN Working Group on Mercenaries, this 'dissociation' of cyberoperations from the states that coordinate them makes it difficult to identify the responsible entities, the scope of the operations, their material and temporal dimensions, unlike what happens in the case of kinetic military or paramilitary operations.

Considering the technical and legal challenges in gathering evidence to attribute the actions of hacker groups to a state, a 'overall digital control' regime would be advisable[68]. This regime relies on the degree of the organization and coordination of the entire cyber-operation, and it is in line with the UN non-binding norms which states that, for the purposes of attributing cyber incidents, states should consider «all relevant information, including the larger context of the event, the challenges of attribution in the Information and Communication Technology (ICT) environment, and the nature and extent of the consequences» (para. 13, letter b)[69].

In this vein, the 2021 GGE report acknowledges the complex nature of the attribution process, noting that «a broad range of factors should be considered before establishing the source of an ICT incident»[70]. The report adds that these factors must be substantiated by factual elements related to the extent and technical characteristics of the operation, its target, the impact on international peace and security, and the outcome of consultations between states, with particular regard to the obligation of peaceful resolution of international disputes.

This might have been the outcome of the attribution to Iran of the cyber-attacks to Albania that, after attributing them to Iran, preferred to declare members of the Iranian diplomatic corps *personae non grata*, rather than reacting in self-defense, probably due to uncertainty

[68] See C. ANTONOPOULOS, *State Responsibility in Cyberspace*, cit., 123, for whom attribution may rest on a presumption that introduces a reversal of the burden of proof.

[69] See OEWG *Report 2021*, cit., 7.

[70] See GEE *Report 2021*, cit., parr. 23-25.

in evidence[71]. This response aligns with the caution advised by the GGE within the UN, to avoid the risk of military escalation between states[72].

7. The evolving landscape of cyberoperations and the increasing offensive capabilities of non-state actors necessitate an adaptive approach by international cyber law. The traditional understanding of armed attacks, rooted in the physical effects of armed force as outlined in the UN Charter, must evolve to encompass the complex and often intangible damages caused by cyber activities. This includes the disruption of critical infrastructures, alteration and cancellation of digital data, and the potential for widespread harm to national security and to international peace and security[73].

To address these challenges, a new multidimensional concept of armed attack in cyber space is essential. This concept should also account for emerging threats such as the malicious use of artificial intelligence and hybrid warfare[74]. It is also necessary to draft an international regulatory framework to hold the private military companies accountable for their illicit activities[75]. This framework should also provide guidelines on the pertaining jurisdiction.

Additionally, the development of a detailed taxonomy of cyber-attacks and clear attribution criteria is crucial. Such criteria should be based on uniform and impartial evidentiary standards to support fair and accurate attribution.

This will ensure a transparent and credible attribution process that will facilitate a global understanding of state practices in cyberspace. Moreover, the UN's initiative to create specific discussion subgroups and Points of Contact (PoC) directories will enhance cooperation and

---

[71] See DEUTSCHE WELLE, *Albania Blames Iran for Cyberattacks*, 16 September, 2022, https://www.dw.com; https://www.reuters.com/world/albania-cuts-iran-ties-orders-diplomats-go-after-cyber-attack-pm-says-2022-09-07/.

[72] See GEE *Report 2021*, cit., par. 22 ff and 71 (g).

[73] See G. CORN, *Sovereignty in the Age of Cyber*, in *American Journal of International Law Unbound*, 2018, 207; P. MICHAEL, F. ISCHERKELLER, *Cyber Persistence Theory: Redefining National Security in Cyberspace*, 2023, https://ndupress.ndu.edu.

[74] SEE OEWG *Report 2022*, cit., parr. 15, a), and 9. On this topic see F.G. HOFFMAN, *Conflict in the 21st Century: The Rise of Hybrid Wars*, 2007, www.potomacinstitute.org; M. CLARK, *Russian Hybrid Warfare*, 2020, https://www.understandingwar.org; G. SIMONS, Y. DANYKM, T. MALIARCHUK, *Hybrid War And Cyber-Attacks: Creating Legal and Operational Dilemmas*, *Global Change*, in *Peace & Security*, 2020, 337 ff; NATO, *NATO's Response to Hybrid Threats*, 2021, www.nato.int.

[75] See OEWG, *Report 2024*, cit., 2.

coordination among states, reducing the risk of misunderstandings and unintended escalations of incidents in international crisis in cyber space[76]. On this topic the OEWG suggests the use by states of multilateral, regional, bilateral platforms to share information on national approaches to attribution, including how states can distinguish between different types of attribution, and ICTs' threats and incidents[77].

It is worth noting the recent proposal of the Program of Action by the UN, along with the suggestion for a Permanent Mechanism by the OEWG's Chair, that underscores the need for continuous dialogue and regulatory oversight[78]. These initiatives aim to establish a robust framework for the application of international law in the context of ICTs use, particularly in response to state-attributable malicious cyber activities.

In conclusion, the international community must work towards developing a uniform legal framework in completion with the recently adopted UN convention against cybercrime[79]. In the meantime, by operationalizing the UN non-binding norms on responsible behavior in cyberspace, states can effectively and efficiently enhance cybersecurity and promote international peace and security in the digital domain[80].

In this context, it is essential to consider the positions of non-Western countries governing the conduct in cyber space because the predictability of states' behavior might clarify the consequences of

[76] See GEE, *Report 2021*, cit., para 77 ff; OEWG, *Report 2022*, cit., 5.

[77] See Letter from OEWG Chair of May 29, 2024. Let it permitted to cite A.L. SCIACOVELLI, *Reflexions on the Hostile Activities in Cyberspace and the International Legal Landscape Promoted by the United Nations*, in *Osservatorio sulle attività delle organizzazioni internazionali e sovranazionali, universali e regionali, sui temi di interesse della politica estera italiana OSORIN*, 2024, www.osorin.it.

[78] Letter from the Chair of the OEWG on Security of and in the Use of Information and Communications Technologies, 2021-2025, February 20, 2024, 6. On this aspects see B. ALERIANO, B. JENSEN, *De-escalation Pathways and Disruptive Technology: Cyber Operations as Off-Ramps to War*, in S. Shackelford, F. DOUZET, C. ANKERSEN (eds.), *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*, Cambridge, 2022, 64-93; M. WALZER, *Cyber Warfare, Media Warfare, and Lawfare*, in M. GROSS, T. MEISELS (eds.), *Soft War: The Ethics of Unarmed Conflict*, Cambridge, 2017, 77 ff.

[79] See UN General Assembly, UN Convention Against Cybercrime, August 7, 2024, UN Doc. A/AC.291/L.15.

[80] GEE, *Official Compendium of Voluntary National Contributions*, cit.; UN *Program of Action to Advance Responsible State Behavior in the Use of Information and Communications Technologies in the Context of International Security*, October 13, 2022, UN Doc. A/C.1/77/L.73. See K. MAČÁK, F*rom Cyber Norms to Cyber Rules: Re-engaging States as Law-Makers*, in *Leiden Journal of International Law*, 2017, 879.

unlawful state behavior in cyberspace and reduce the risk of miscalculation in attributing cyber activities.