International Journal of Law and Politics Studies
ISSN: 2709-0914
DOI: 10.32996/ijlps
Journal Homepage: www.al-kindipublisher.com/index.php/ijlps

IJLPS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Cybercrimes: An Emerging Category of Offenses within the Frame of the International Criminal Court Jurisdiction

Clara Pettoello-Mantovani, JD, LLM
Law Firm R.Romeo, Rome, Italy and LUISS University, Master Course in Cybersecurity, Rome, Italy
Corresponding Author: Clara Pettoello-Mantovani, JD, LLM, **E-mail**: c.pettoellomantovani@gmail.com

| ABSTRACT
In our interconnected society, crime persists, demanding joint efforts by national and international authorities to detect, prevent, and prosecute criminal activities. Jurisprudential evolution mandates lawmakers to possess a comprehensive legal vision, adapting laws to changing social contexts and emerging criminal methods, especially in technology, including computer technology and Artificial Intelligence (AI). This article comments on the escalating vulnerability of sovereign states and their economies to cyber-attacks. The radical evolution of computer systems has led to new modes of aggression, targeting not only traditional legal assets but also individuals familiar with advanced technology. The emergence of "cyberwarfare" prompts inquiries into potential categorizations within international legal frameworks. Recent global conflicts highlight the potential classification of cyber-attacks on critical infrastructure as war crimes or acts of aggression, urging the International Criminal Court (ICC) to consider incorporating cybercrimes into its core interests. While normative references may lack in existing conventions, the Martens Clause emphasizes treating attacks using technology as equivalent to conventional means. Article 51 of the United Nations Charter implies that cyber weapons could be deemed equivalent to conventional weapons under international law. The article stresses the importance of education and advanced training for legal personnel skilled in identifying cybercrime perpetrators, challenging the ICC to recruit or train individuals with the necessary legal and technical expertise for effective cybersecurity responses. The article briefly explores challenges in conceptualizing and categorizing cybercrimes within existing legal frameworks. The intersection of law and technology necessitates harmonious collaboration between legal and technical experts, acknowledging the intricate web of cyberspace and the implications of cyber threats on global stability and security. In conclusion, the article advocates a fundamental shift in the approach to justice, recognizing the ICC's imperative evolution in addressing cybercrimes. Integrating cybercrimes into the ICC's purview aligns with international law principles, emphasizing the equivalence of cyber weapons to conventional arms. Collaboration between legal and technical experts is essential in navigating the complexities of cybercrimes, ensuring accountability, and upholding justice in the digital age. The article concludes by highlighting the proactive role of the ICC in shaping the future of global justice amid emerging cyber threats.

| KEYWORDS

Cybercrimes, Artificial Intelligence, International Criminal Court, Jurisdiction, Computer, Attaks.

| ARTICLE INFORMATION

ACCEPTED: 12 February 2024 **PUBLISHED:** 13 March 2024 **DOI:** 10.32996/ijlps.2024.6.2.2

1. Introduction

Crime, deeply embedded in our society, persists as an intrinsic element, necessitating diligent efforts by national and international authorities to uncover, preempt, and prosecute criminal activities in all their forms. The pursuit of justice is demanding, requiring

legislators to possess a comprehensive legal vision and broad mental flexibility to keep pace with constantly evolving jurisprudence[1,2]

The continual adaptation of laws and regulations is crucial to ensure they remain rational and responsive to changes in social contexts and the evolution of new forms and methods through which criminal activities manifest. Technological advancements, particularly in computer technology and Artificial Intelligence (AI), represent a major development in national and international scenarios where criminal activities unfold[3,4].

2. Unveiling the vulnerability: interconnected computer systems and AI tools in the face of cyber-attacks

The increasing importance of interconnected computer systems and AI tools has rendered sovereign states and their economies vulnerable to cyber-attacks, from third countries or terrorist groups with strategic objectives. In the face of the radical evolution of computer systems and data manipulation techniques on computer networks, new modes of aggression have inevitably emerged[3].

These modes of aggression not only target traditional legal assets of private and public nature, namely industry and nations, but also individuals born and developed in tandem with the proliferation of computer systems, presumably familiar with the various forms of advanced technology[4].

In this context, progressively more dangerous and effective modes of aggression have developed, leading to the formulation of techniques and tactics of actual "cyberwarfare." These are aimed at compromising the defenses and military capabilities of a nation or even the functioning of entire countries, shifting the theater of conflicts into a "fifth dimension" alongside the traditional ones of land, sea, sky, and space[3].

Amidst the rising prevalence of emerging cyber threats, the utilization of the 'metaverse' presents a concerning risk capable of inflicting severe damage on a nation's vital strategic infrastructures. High-impact intrusion or sabotage techniques on the computer or telecommunications networks of an adversary country, in a context of war, define "cyberwarfare," aiming to compromise the defenses, functioning, and even the economic and socio-political stability of the opponent.

The prospect of incorporating cyberspace into the realm of international relations through the use of force has sparked intriguing inquiries regarding the potential categorization of cyberwarfare within international legal frameworks[5].

In view of recent global conflicts, it appears clear that potential cyber-attacks on critical strategic infrastructure, as well as non-military, civil targets, are actions attributable as war crimes and/or acts of aggression[5]. Hence, it is of primary importance for the International Criminal Court (ICC) to contemplate incorporating into its core interests and emerging objectives the analysis and investigation of the burgeoning legal cases associated with "cybercrimes." Such an approach appears to align seamlessly with the scope of crimes within the jurisdiction of the International Criminal Court, as outlined in Article 2, Part 5 of its statute[6].

While specific normative references within the IV Hague Convention and major international conventions on humanitarian law may lack discussion on the topic of cybercrimes, the Martens Clause in the convention's preamble underscores the urgency of considering attacks using technology as equivalent to those conducted through conventional means[7].

Supporting this legal view, we can turn to Article 51 of the United Nations Charter, which prohibits the use of force irrespective of the weapon employed[8]. This implicitly asserts that a cyber weapon could be deemed equivalent to a conventional weapon under international law. Consequently, customary and treaty international law becomes directly applicable in the event of a cyberattack[8].

[1] Soafer A.D., Goodman S.E., (2005) The Transnational Dimension of Cyber Crime and Terrorism, Hoover Press,

[2] Picotti L. (2020) Cybercrime e tutela penale dei diritti della persona e della privacy nel web, AIAF, pp.7-15.

[3] Bellacosa M. (2024) The place of consumption of the crime of unauthorized access to a computer or telematic system: awaiting the joint sections. Available at: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://archiviodpc.dirittopenaleuomo.org/upload/1422829558BELLACOSA_2015a.pdf

[4] Pettoello-Mantovani C. (2022) Cybersecurity in the current framework of the EU and Italian criminal justice systems. A focus on digital identity theft. Monograph, Nova Science Publishers, New York, USA

[5] Grabrosky P.N., 2004 Global Dimension of Cybercrime, Global Crime, Press.

[6] International Criminal Court (ICC). (2024) Court records and transcripts, Available at: https://www.icc-cpi.int/documents

[7] International Humanitarian Law Databases. Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 18 October 1907. Available at: https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-iv-1907

[8] United Nations. Repertory of practice of United Nations organs. Available at: https://legal.un.org/repertory/art51.shtml

The education and advanced training programs of legal personnel skilled in identifying specific perpetrators of cybercrimes become of fundamental importance. Therefore, the challenge in the coming years will be for the International Criminal Court to recruit or train individuals with the necessary legal and technical expertise and skills to work on cases related to cybersecurity and cybercrimes[9].

3. Delving further into the intricate domain of cybercrimes.

As we delve deeper into the multifaceted realm of cybercrimes, it becomes imperative to explore the intricate challenges and implications that this evolving landscape brings to the forefront of international law. The notion of "cyberwarfare" introduces a paradigm shift, expanding the traditional dimensions of conflicts and prompting legal scholars, policymakers, and international organizations to grapple with the intricacies of this digital battleground[4].

One of the key challenges lies in the conceptualization and categorization of cybercrimes within existing legal frameworks. While conventional laws have been adept at addressing crimes in the physical realm, the intangible nature of cybercrimes demands a nuanced understanding and adaptation of legal doctrines. The question arises: How can we effectively apply age-old principles of international law to combat and prosecute crimes that unfold in the intricate web of cyberspace?

The evolving landscape of cyber threats necessitates a holistic approach, intertwining legal, technological, and diplomatic efforts[10]. The sophisticated techniques employed by cybercriminals, often crossing international borders seamlessly, emphasize the need for a collaborative and globally coordinated response. In this context, the role of the International Criminal Court becomes pivotal, as it becomes the arena where the legal ramifications of cybercrimes are deliberated and adjudicated[11].

The traditional understanding of warfare, confined to physical battlegrounds, has undergone a profound transformation with the advent of cyberwarfare. As nations and entities engage in a perpetual struggle for dominance in the digital sphere, the repercussions extend far beyond the virtual realm. Critical infrastructures, ranging from power grids to financial systems, are now vulnerable to malicious cyber activities, blurring the lines between conventional warfare and cyber threats.

The emergence of the 'metaverse' further complicates the landscape, introducing a virtual space where the potential for cyber-attacks transcends the boundaries of conventional understanding. The International Criminal Court must adapt its strategies to encompass these novel challenges, recognizing that the impact of cybercrimes extends beyond the physical to the very fabric of a nation's stability and security[11].

In the realm of international relations, the consideration of cybercrimes as war crimes or acts of aggression prompts a reevaluation of existing legal doctrines. The Martens Clause, embedded in the IV Hague Convention[7], becomes a guiding principle, urging the acknowledgment of technological advancements as equivalent to conventional means of warfare. As commented above, this recognition is echoed in Article 51 of the United Nations Charter, underscoring the prohibition of the use of force regardless of the type of weapon utilized[8].

The implications of these legal frameworks extend beyond theoretical considerations, influencing the practical approach to investigating and prosecuting cybercrimes. As the ICC grapples with the inclusion of cybercrimes within its jurisdiction, the need for specialized knowledge becomes paramount. Legal personnel equipped with both legal expertise and technical acumen are essential to navigate the complexities of cyber investigations and prosecutions.

4. Adapting Justice to the Transforming Landscape of Cyber Threats

The evolving nature of cyber threats demands a proactive approach, anticipating future challenges and adapting legal frameworks accordingly. The International Criminal Court must become a dynamic institution, capable of staying ahead of the curve in a landscape where technology evolves at an unprecedented pace. Educational and training programs should focus on cultivating a cadre of experts who can unravel the intricacies of cybercrimes, identify specific perpetrators, and ensure accountability within the bounds of international law.

[9] Severino P., (2020) "Cybersecurity: Regulation and Policy," Luiss Law School seminar, 2019-2020.LUISS Press, Rome

[10] Picotti L, (2020) Online child pornography offences. A brief overview, in Festschrift fur Frieder Dunkel zum 70. (2020) Kriminologie und Kriminalpolitik im Dienste der Menschenwürde, Forum Verlag Godesberg, Monchengladback, 2020, pp. 207-208

[11] International Criminal Court (ICC) (2024) Statement by ICC Prosecutor Karim A.A. Khan KC on conference addressing cyber-enabled crimes through the Rome Statute system. Available on: https://www.icc-cpi.int/news/statement-icc-prosecutor-karim-aa-khan-kc-conference-addressing-cyber-enabled-crimes-through

The fusion of crime and technology in our interconnected world necessitates a paradigm shift in the approach to justice[4]. The International Criminal Court, as a guardian of global justice, must evolve to address the challenges posed by cybercrimes. The integration of cybercrimes within its purview aligns with the foundational principles of international law, emphasizing the equivalence of cyber weapons to conventional arms. As we stand at the intersection of law and technology, the harmonious collaboration between legal and technical experts becomes indispensable in the pursuit of justice in the digital age[12].

5. Conclusion

In drawing our conclusions, it becomes increasingly evident that the convergence of crime and technology in our globally interconnected world demands a profound paradigm shift in the traditional approach to justice. The International Criminal Court, standing as a sentinel of global justice, must undergo a transformative evolution to effectively grapple with the multifaceted challenges presented by the rapidly evolving landscape of cybercrimes. This evolution is not merely a matter of necessity but a crucial imperative to ensure that the principles of justice and accountability extend seamlessly into the digital realm.

The imperative to integrate cybercrimes within the purview of the International Criminal Court arises from a meticulous examination of the foundational principles of international law. In this context, the equivalence of cyber weapons to their conventional counterparts emerges as a guiding principle. The understanding that a cyber weapon possesses the potential for equivalent harm as a traditional armament underscores the urgency for the International Criminal Court to broaden its scope. This expansion is not only in response to the undeniable reality of cyber threats but is also a proactive measure to align international legal frameworks with the evolving nature of conflict in the digital age.

At the intersection of law and technology, we find ourselves navigating uncharted territory. The harmonious collaboration between legal and technical experts emerges as an indispensable factor in the pursuit of justice in this digital age. The complexity of cybercrimes requires a unique synergy between legal acumen and technical expertise to unravel the intricate web of digital evidence, identify perpetrators, and navigate the labyrinthine landscapes of cyberspace. The International Criminal Court, in recognizing the gravity of cybercrimes, must prioritize the cultivation of a cadre of professionals adept in both legal intricacies and technological nuances.

Moreover, the current global landscape, marked by geopolitical tensions and the increasing prevalence of cyber threats, necessitates the International Criminal Court's proactive stance in adapting to contemporary challenges. The inclusion of cybercrimes within its purview not only fortifies the Court's relevance but also serves as a deterrent against the impunity that perpetrators of cybercrimes might otherwise enjoy. This evolution is imperative for maintaining the integrity of the global justice system and upholding the principles of accountability and responsibility in the face of emerging threats.

As we look toward the future, it is evident that the International Criminal Court's role in addressing cybercrimes is pivotal. The Court must not only adapt its legal frameworks but also engage in robust educational initiatives to equip legal professionals with the skills necessary to tackle the complexities of cyber investigations. The integration of cybercrimes into the International Criminal Court's mandate represents a proactive and forward-looking approach, ensuring that justice transcends the physical boundaries of traditional warfare and extends its reach into the virtual realm.

In conclusion, the synergy between crime and technology necessitates a reimagining of justice, and the International Criminal Court stands at the forefront of this transformative journey. The integration of cybercrimes into its mandate is not just an acknowledgment of the present challenges but a commitment to shaping the future of global justice in the digital age. The harmonious collaboration between legal and technical experts, the alignment with foundational principles of international law, and the proactive adaptation to emerging threats define the path forward for the International Criminal Court in its pursuit of justice on the global stage.

6. Study Limitations and Future Research

The article primarily focuses on the intersection of cybercrimes and international law, specifically emphasizing the role of the International Criminal Court (ICC). However, the commentary does not extensively explore potential regional variations in legal frameworks or the perspectives of individual nations, as it was beyond the scope of the discussion. Another limitation is associated with the rapid evolution of technology and the legal landscape, particularly in the realm of cybercrimes, which may render certain aspects of the discussion time-sensitive. Therefore, readers should consider this article in the context of its time of writing, as

[12] European Union Commission. The European Agenda on Security. Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions. EU Edition, Strasbourg, 28.04.2015 – COM(2015) 185final. Available on: https://ec.europa.eu/home-affairs/sites/default/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf.

developments since then may impact its relevance. Furthermore, it's crucial to recognize that the effectiveness of the ICC's initiatives in addressing cybercrimes may be influenced by the availability of resources, both in terms of funding and technological infrastructure. Several key factors underscore the significance of these resources in shaping the ICC's ability to effectively tackle cybercrimes, including expertise and training. Combatting cybercrimes demands a high level of technical expertise and specialized knowledge.

Another limiting factor hindering effective action by the ICC and impacting on the analysis presented in this article, is the lack of technological capabilities. The nature of cybercrimes often involves sophisticated technologies and techniques. To investigate and prosecute cybercriminals, the ICC needs state-of-the-art technological tools and infrastructure. This includes advanced forensic software, secure communication channels, and robust cybersecurity measures. Limited funding can impede the acquisition and maintenance of these technologies, hindering the ICC's ability to keep pace with evolving cyber threats. Insufficient international collaboration is an additional limiting factor which also influenced the debate on the issues discussed by the article. Cybercrimes frequently transcend national borders, necessitating international cooperation. The ICC relies on collaboration with national authorities, law enforcement agencies, and technology experts from various countries. Adequate funding is therefore not only important for the improvement of technological equipment and infrastructures, but also essential for establishing and maintaining partnerships, facilitating information exchange, and coordinating efforts on a global scale. Without sufficient resources, the ICC may struggle to foster the necessary international alliances to effectively combat cybercrimes. The landscape of cyber threats is dynamic, with new tactics and technologies continually emerging. A well-funded ICC can invest in ongoing research and development to stay ahead of cybercriminalsand less vulnerable to rapidly evolving cyber threats. Finally, effective responses to cybercrimes also involve raising public awareness and educating individuals about cybersecurity. This requires funding for public awareness campaigns, educational programs, and initiatives to promote responsible online behavior. Therefore, limited resources may also hinder the ICC's capacity to engage in comprehensive outreach efforts to prevent cybercrimes and encourage cooperation from the public.

In summary, a significant limitation of this article relates to the challenge of effectively discussing the ICC's ability to combat cybercrimes, which, however, is intricately tied to the availability of resources. Adequate funding and technological infrastructure are essential for building expertise, acquiring advanced tools, fostering international collaboration, staying informed about emerging threats, developing legal frameworks, and promoting public awareness. Insufficient resources can compromise the ICC's ability to navigate the complex and rapidly evolving landscape of cybercrimes, limiting its impact in this critical area of global justice.

Possible future research directions in the area discussed by the text could include an analysis and investigation of the existing legal frameworks related to cybercrimes at the regional level. This involves exploring how different regions address cybercrimes and identifying potential variations in legal approaches and perspectives among nations. Another crucial area for future research is the impact of technological evolution on legal responses. This entails studying how the rapid evolution of technology affects legal responses to cybercrimes. Additionally, it involves exploring innovative technological solutions for enhancing cyber investigations, including advancements in digital forensics, cybersecurity tools, and artificial intelligence that can assist in identifying specific perpetrators of cybercrimes. These areas of research are closely tied to evaluating how legal systems adapt to new technological developments and the importance of assessing the effectiveness of these adaptations in addressing emerging cyber threats. It is also essential to delve into the dynamics of international collaboration in combating cybercrimes, emphasizing the significance of successful collaborative efforts between nations, law enforcement agencies, and international organizations.

A strategically important area of research includes examining the implications of recent global conflicts and cyber-attacks on critical infrastructures. This entails investigating whether such actions should be formally classified as war crimes or acts of aggression. Another critical focus for future research involves anticipating and analyzing future trends in cyber threats. This includes studying emerging techniques and tactics employed by cybercriminals and assessing how these trends may shape the landscape of international law and the strategies employed by legal bodies to address cybercrimes.

A final key area of research should be dedicated to the capacity building for legal personnel and developing strategies to enhance their capacity to handle cyber investigations. This is of paramount importance, and there is a need to create educational and training programs that can equip legal professionals with both legal expertise and technical acumen to navigate the complexities of cybercrimes effectively. These research directions can contribute to a more comprehensive understanding of the evolving intersection between cybercrimes and international law, guiding policymakers, legal practitioners, and technologists in developing effective strategies to address the challenges presented by the digital age.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
ORCID: https://orcid.org/0000-0002-6117-0631
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Bellacosa M. (2024) The place of consumption of the crime of unauthorized access to a computer or telematic system: awaiting the joint sections. Available at: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://archiviodpc.dirittopenaleuomo.org/upload/1422829558BELLACOSA_2015a.pdf
[2] European Union Commission (2015). The European Agenda on Security. Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions. EU Edition, Strasbourg, 28.04.2015 – COM(2015) 185final. Available on: https://ec.europa.eu/home-affairs/sites/default/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf.
[3] Grabrosky P.N., (2004). Global Dimension of Cybercrime, Global Crime. Geneva, Switzerland
[4] International Criminal Court (ICC). (2024) Court records and transcripts, Available at: https://www.icc-cpi.int/documents
[5] International Criminal Court (ICC) (2024) Statement by ICC Prosecutor Karim A.A. Khan KC on conference addressing cyber-enabled crimes through the Rome Statute system. Available on: https://www.icc-cpi.int/news/statement-icc-prosecutor-karim-aa-khan-kc-conference-addressing-cyber-enabled-crimes-through
[6] International Humanitarian Law Databases. Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 18 October 1907. Available at: https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-iv-1907
[7] Pettoello-Mantovani C. (2022) Cybersecurity in the current framework of the EU and Italian criminal justice systems. A focus on digital identity theft. Monograph, Nova Science Publishers, New York, USA
[8] Picotti L. (2020). Cybercrime e tutela penale dei diritti della persona e della privacy nel web, AIAF, pp.7-15, AIAF, Verona, Italy
[9] Picotti L, (2020). Online child pornography offences. A brief overview, in Festschrift fur Frieder Dunkel zum 70. (2020) Kriminologie und Kriminalpolitik im Dienste der Menschenwürde, Forum Verlag Godesberg, 2020, pp. 207-208. Monchengladback, Germany
[10] Severino P., (2020). Cybersecurity: Regulation and Policy, Luiss Law School seminar, 2019-2020.LUISS Press, Rome, Italy
[11] Soafer A.D., Goodman S.E., (2005). The Transnational Dimension of Cyber Crime and Terrorism, Hoover Press, Stanford, CA. USA
[12] United Nations. Repertory of practice of United Nations organs. Available at: https://legal.un.org/repertory/art51.shtml