The17th Year Publication, No.1

June 2025

GLOBAL SECURITY AND CYBERCRIME: AN IN-DEPTH ANALYSIS

Orinda Malltezi*

*Faculty of Social Sciences , Albanian University

Abstract

Cybercrimes have increased a lot in the international arena and to date there is no international institution to take actions on the increasing number of cybercrimes. However, this concern exists for all countries in the world that face cyberattacks on a daily basis. This is a new phenomenon for all countries as a result of the increased use of the internet and the purchases that we make especially on websites anywhere in the world. Attention to cybercrimes has increased everywhere in every country in the world, the countries of the Global North have greater protection in terms of cybercrimes than the Global South, but now cybercrime knows no borders and becomes difficult to catch. What happens to all the information that is requested from us by different websites like Amazon when we buy a new product? Do they store our address, credit card, card number, and phone number on a secure and encrypted server? When you Accept User Agreement for iTunes, which you obviously don't read, what protections does Apple offer to keep your information safe? Yes, consumers increasingly use the internet to make everyday purchases and businesses increasingly collect and store consumer information. Safeguards must be put in place to ensure that this information is stored in a way that limits and prevents cybercrime threats. An October 2015 study by the Ponemon Institute determined that the average annual cost of cybercrime in the United States is $15.42 million for United States Companies – an increase from $12.69 million just a year ago.' As the threat of cybersecurity breaches to consumers continues to grow, and the costs associated with this threat continue to rise, businesses must find ways to protect consumers. How Countries will deal with the rise of cybercrime when there is no international organization that examines or regulates legislation regarding cybercrimes that know no borders? As happened with the taking of personal data of individuals in Albania from Iranian attacks for which no one was held responsible and leaving millions of citizens exposed to the use of their personal data on various websites or for various other crimes. Should there be higher security regarding cybercrimes in every country in the world, including Albania, in order to protect consumers or citizens who may fall prey to the use of their personal data by criminals? Should the relevant institutions have a more active role in this regard? These are some of the questions that this paper tries to answer.

Key words: *Cybercrime, internet, relevant institutions, technology, state policy*

Introduction

The rapid expansion of global digital networks has revolutionized economic, social, and political interactions worldwide. While globalization fosters innovation and connectivity, it has simultaneously heightened vulnerabilities to cybercrime, a pervasive and rapidly evolving threat. This paper explores the multifaceted nature of cybercrime, examines its impact on global security, and highlights the critical need for international cooperation and legal harmonization to effectively counter cyber threats.

The increasing dependence on information and communication technologies (ICTs) for critical infrastructure, commerce, governance, and daily life creates expansive attack surfaces for cyber adversaries[1].

Cybercriminals, ranging from lone hackers to organized syndicates and state-sponsored actors, exploit weaknesses for financial gain, political influence, espionage, or disruption.

Cybercrime transcends national boundaries, complicating enforcement and prevention efforts. It presents formidable challenges to governments and private sectors alike, particularly in developing countries that lack sufficient cybersecurity infrastructure[2]. As cyber threats escalate in frequency, complexity, and impact, there is a growing consensus that collective international action is essential to safeguard economies, security, and democratic institutions[3].

The Evolution of Cybercrime

Cybercrime has evolved from isolated, relatively unsophisticated attacks to highly organized, global criminal enterprises. Early hacking in the 1980s and 1990s was often driven by curiosity or notoriety, but by the 2000s, cybercrime shifted toward monetization. Cybercriminals began leveraging malware, ransomware, and phishing to steal personal information, corporate secrets, and government data[4].

The proliferation of mobile devices, cloud computing, and Internet of Things (IoT) technologies has further expanded the cyber threat landscape. Each new technology introduces vulnerabilities and new avenues for exploitation. The growing adoption of cryptocurrencies has also facilitated illicit transactions by obscuring payment trails[5].

State-sponsored cyber operations now blur the lines between criminality and geopolitical conflict. Countries employ cyber capabilities for espionage, sabotage, and influence campaigns, complicating international relations and raising the specter of cyber warfare[6]. Incidents like the 2017 WannaCry ransomware attack demonstrated how cyber weapons could disrupt critical services worldwide, from healthcare to transportation.

Forms and Techniques of Cybercrime

Cybercrime encompasses a diverse set of illicit activities:

1. Hacking and Unauthorized Access

Hackers exploit vulnerabilities in software or network configurations to gain unauthorized access. Techniques include brute-force attacks, SQL injections, and exploiting zero-day vulnerabilities—unknown flaws for which no patches exist[8]. Once inside, attackers may install backdoors, exfiltrate data, or manipulate systems.

2. Malware and Ransomware

Malware—malicious software—includes viruses, worms, Trojans, spyware, and ransomware. Ransomware encrypts victims' data, demanding payment for decryption keys. Attacks on hospitals, municipalities, and businesses using ransomware have surged in recent years[9].

3. Phishing and Social Engineering

Phishing uses fraudulent emails or messages to trick users into revealing sensitive information or installing malware. Social engineering exploits human psychology rather than technical vulnerabilities, making it a persistent and effective attack vector[10].

4. Distributed Denial of Service (DDoS) Attacks

Attackers overwhelm servers or networks with traffic, disrupting services. DDoS attacks can be used for extortion, political protest, or as smokescreens to distract security teams during other attacks[11].

5. Cyber Espionage and State-Sponsored Attacks

Intelligence agencies and nation-states conduct cyber espionage to gather political, economic, or military

secrets. Advanced Persistent Threats (APTs) involve prolonged, stealthy intrusions targeting sensitive information[12].

6. Financial Cybercrime

This includes credit card fraud, identity theft, and online banking fraud. Cybercriminals exploit weaknesses in payment systems or manipulate markets through insider trading enabled by hacked data[13].

Impact of Cybercrime on Global Security

Cybercrime poses serious risks beyond immediate financial loss. Critical infrastructure—including power grids, telecommunications, healthcare, and financial systems—is increasingly targeted. Disruptions in these sectors can have cascading effects on national security and public safety[14].

For instance, the 2015 cyberattack on Ukraine's power grid caused widespread blackouts and demonstrated how cyber operations could destabilize civilian infrastructure[15]. Similarly, attacks on financial markets, such as the 2016 Bangladesh Bank heist where $81 million was stolen via the SWIFT banking network, threaten economic stability[16].

The social impact is profound. Public trust in institutions erodes when personal data is compromised or services are disrupted. Cybercrime also affects democratic processes, as misinformation campaigns and election interference have shown in multiple countries[17].

Developing countries face disproportionate challenges due to limited resources and infrastructure. Their increasing digitalization creates new vulnerabilities without commensurate security investments[18]. This asymmetry offers cybercriminals opportunities to exploit weak links and serves as a reminder that global cybersecurity is only as strong as its weakest participant.

Geographic Distribution of Cybercrime

Cybercrime hotspots correspond to regions with significant digital infrastructure but varied cybersecurity maturity. North America, Europe, and East Asia face the highest volumes of attacks, while developing regions are increasingly targeted due to weaker defenses.**Chart 1: Cybercrime Incidents by Region (2023)**

Region	% of Global Incidents
North America	40%
Europe	30%
Asia-Pacific	20%
Latin America	5%
Africa	3%
Middle East	2%

Legal and Regulatory Challenges

One of the most significant obstacles to combating cybercrime is the lack of a unified global legal framework. Different countries have different definitions, standards, and enforcement capabilities. Some states prioritize cybersecurity, while others may lack political will or technical capacity[19].

The Council of Europe's Budapest Convention on Cybercrime (2001) is the first major international treaty addressing cybercrime. It establishes standards for criminalization, investigation, and international cooperation[20]. However, not all countries have ratified it, and some major powers like Russia and China remain outside its framework, citing sovereignty concerns[21].

National laws often struggle to keep pace with technology. Cybercrime statutes vary widely, complicating cross-border investigations. Mutual legal assistance treaties (MLATs) are often slow, bureaucratic, and inadequate for timely responses to rapidly unfolding cyber incidents[22].

Privacy regulations such as the EU's General Data Protection Regulation (GDPR) introduce obligations for data protection, breach notification, and user rights, but also increase compliance complexity for multinational companies[23].

The export controls on cybersecurity products and cryptography pose additional dilemmas, balancing national security with global trade and cooperation[24].

International Cooperation Efforts

Recognizing the transnational nature of cybercrime, various international bodies coordinate efforts:

- The United Nations Office on Drugs and Crime (UNODC) supports capacity building and promotes legal frameworks[25].
- Interpol facilitates information sharing and joint operations against cybercrime syndicates[26].
- The International Telecommunication Union (ITU) works on standards and capacity development[27].
- The G7 and G20 include cybersecurity in their strategic discussions[28].

Despite these initiatives, geopolitical rivalries and divergent national interests often impede progress. Cyber sovereignty, differing views on internet governance, and concerns over surveillance complicate trust and collaboration[29].

The Role of the Private Sector

Given that much critical infrastructure and data reside in the private sector, businesses are frontline defenders against cyber threats. Many organizations lack sufficient resources or expertise to combat sophisticated cyberattacks[30].

Public-private partnerships are increasingly essential. Information sharing platforms, joint threat intelligence, and coordinated incident response enhance resilience. Industry standards and best practices, such as the NIST Cybersecurity Framework, provide valuable guidance[31].

However, challenges remain in incentivizing transparency, balancing privacy concerns, and ensuring global standards across industries and jurisdictions[32].**Emerging Threats and Future Trends**

Cyber threats continue to evolve with technology. Artificial intelligence (AI) and machine learning enable more sophisticated attacks and defense mechanisms[33]. Quantum computing poses potential risks to current cryptographic systems, necessitating future-proofing encryption[34].

The expansion of 5G networks and IoT devices creates new attack vectors. Securing the "smart city" infrastructure and autonomous systems is critical[35].

Supply chain attacks—where attackers compromise trusted third-party vendors—have emerged as a major concern, exemplified by the 2020 SolarWinds breach affecting numerous governments and corporations[36].**Recommendations and Conclusion**

Cybercrime today represents one of the most complex and pressing challenges to global security, economic stability, and societal trust in the digital age. The scope and sophistication of cyberattacks continue to expand, fueled by rapid technological innovation, increasing interconnectivity, and geopolitical rivalries. This paper has demonstrated that no single nation, institution, or sector can combat cybercrime effectively in isolation. Instead, a multifaceted and collaborative approach is essential.

Firstly, the **nature of cybercrime** has evolved beyond petty hacking and phishing to encompass large-scale, state-sponsored espionage, supply chain compromises, and ransomware campaigns that disrupt critical infrastructure. These attacks threaten not only businesses but also national security and public safety. As evidenced by high-profile incidents like the SolarWinds breach and the Colonial Pipeline ran-

somware attack, the economic and social costs can be staggering and far-reaching.

Secondly, **existing legal and regulatory frameworks** face significant limitations. Many countries struggle with outdated laws that fail to keep pace with new cyber threats, while differences in legal definitions and enforcement capabilities create jurisdictional gaps exploited by criminals. Rising nationalism and geopolitical tensions further complicate international cooperation, undermining treaties and global institutions designed to harmonize responses to cybercrime. Moreover, developing countries frequently lack the necessary resources, technical capacity, and institutional support to mount effective defenses, making them disproportionately vulnerable and potentially serving as entry points for transnational cybercriminal networks.

Thirdly, **the rapid evolution of technology** presents both opportunities and risks. Emerging technologies such as artificial intelligence, quantum computing, and the Internet of Things exponentially increase the attack surface while simultaneously offering new tools for detection and defense. This dual-use dilemma requires that policymakers and technologists work closely to anticipate threats, develop resilient systems, and promote secure technology adoption.

Given these realities, the paper highlights several critical priorities moving forward:

1. **Strengthening International Cooperation:** Effective cybercrime mitigation depends on robust, legally binding international agreements that transcend narrow national interests. Efforts must focus on harmonizing definitions of cyber offenses, establishing clear protocols for information sharing, and facilitating joint investigations and prosecutions. Institutions like the United Nations, INTERPOL, and regional bodies must be empowered with adequate resources and political support to coordinate global action.

2. **Building Capacity in Developing Countries:** Bridging the global cybersecurity divide is vital. Investment in education, infrastructure, and institutional reforms in developing nations will reduce vulnerabilities and prevent their exploitation as safe havens. International partnerships and funding mechanisms can catalyze these efforts, fostering inclusive resilience.

3. **Enhancing Public-Private Partnerships:** Since much critical infrastructure and data resides in the private sector, cooperation between governments, industry, and civil society is essential. Transparent sharing of threat intelligence, collaborative incident response, and joint development of cybersecurity standards can significantly improve collective defenses.

4. **Adopting Agile Legal and Regulatory Approaches:** Governments should pursue flexible, technology-neutral legislation that can adapt to evolving threats without stifling innovation. Regulatory frameworks must balance security, privacy, and civil liberties while promoting transparency and accountability.

5. **Prioritizing Research and Innovation:** Continued investment in advanced cybersecurity research—especially in AI-driven defense, quantum-resistant cryptography, and secure IoT design—is necessary to stay ahead of increasingly sophisticated adversaries.

6. **Raising Public Awareness and Education:** Human error remains a leading cause of breaches. Comprehensive, ongoing cybersecurity education for individuals, employees, and leadership will reduce risks and strengthen the overall security posture.

Finally, cybercrime is not merely a technical or legal issue; it is a **strategic geopolitical challenge** that reflects broader dynamics of power and trust in the international system. Managing cyber risks requires not only technological solutions but also diplomatic engagement and confidence-building measures to prevent escalation and foster stability.

In conclusion, combating cybercrime effectively demands a **holistic, coordinated approach** that integrates policy, technology, law enforcement, and international diplomacy. Only through sustained collaboration at all levels—local, national, regional, and global—can the international community hope to secure cyberspace and harness its full potential for the betterment of society.

As conclusion to mitigate cybercrime's growing threat, the following actions are imperative:

1. **Enhance International Legal Harmonization:** Expand adoption of conventions like the Budapest Convention and develop new treaties addressing emerging threats[37].
2. **Increase Capacity Building:** Support developing countries with funding, training, and technology transfer to strengthen cyber defenses[38].
3. **Foster Public-Private Collaboration:** Encourage transparent, timely information sharing and joint response frameworks[39].
4. **Invest in Research and Innovation:** Develop AI-driven cybersecurity tools, quantum-resistant cryptography, and secure IoT architectures[40].
5. **Promote Public Awareness:** Educate individuals and organizations on cybersecurity best practices to reduce human vulnerabilities[41].

In conclusion, cybercrime represents one of the foremost challenges of the 21st century, intersecting technology, law, economics, and geopolitics. The global community must act collectively, innovatively, and decisively to protect the digital commons upon which modern life increasingly depends.

Bibliography

1. Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, 30(8), 719–731.
2. Kshetri, N. (2017). Cybercrime and Cybersecurity in Developing Economies. *IT Professional*, 19(2), 11–14.
3. Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.
4. Mitnick, K. D., & Simon, W. L. (2011). *The Art of Intrusion*. Wiley.
5. Symantec Corporation. (2019). *Internet Security Threat Report*.
6. Libicki, M. C. (2007). *Cyberdeterrence and Cyberwar*. RAND Corporation.
7. Healey, J. (2018). *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Cyber Conflict Studies Association.
8. Brenner, S. W. (2010). *Cybercrime: Criminal Threats from Cyberspace*. Praeger.
9. European Union Agency for Cybersecurity (ENISA). (2022). *Threat Landscape Report*.
10. Hong, J. (2012). The State of Phishing Attacks. *Communications of the ACM*, 55(1), 74–81.
11. Anderson, R., et al. (2013). Measuring the Cost of Cybercrime. *Workshop on the Economics of Information Security*.
12. Office of the Director of National Intelligence. (2020). *Annual Threat Assessment*.
13. PwC. (2017). *Global Economic Crime and Fraud Survey*.
14. US Department of Homeland Security. (2016). *Critical Infrastructure Cybersecurity*.
15. Case, T., & Marczak, B. (2016). Analysis of the Cyberattack on the Ukrainian Power Grid. *SANS ICS Security*.
16. FBI. (2016). Bangladesh Bank Cyber Heist.

17. Bradshaw, S., & Howard, P. N. (2019). The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation. *Computational Propaganda Research Project*.

20. ITU. (2018). *Global Cybersecurity Index*.

21. UN Office on Drugs and Crime. (2013). *Comprehensive Study on Cybercrime*.

22. Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)*.

23. Segal, A. (2016). *The Hacked World Order*. PublicAffairs.

24. Brenner, S. W. (2010). *Cybercrime: Criminal Threats from Cyberspace*. Praeger.

25. European Parliament. (2016). *General Data Protection Regulation (GDPR)*.

26. Segal, A. (2016). *The Hacked World Order*. PublicAffairs.

27. United Nations Office on Drugs and Crime. (2018). *Cybercrime and Cybersecurity*.

28. Interpol. (2020). *Cybercrime Reports and Operations*.

29. ITU. (2021). *Global Cybersecurity Agenda*.

30. G7. (2021). *Cybersecurity and Digital Policy*.

31. Kurbalija, J. (2017). *An Introduction to Internet Governance*. DiploFoundation.

32. Verizon. (2018). *Data Breach Investigations Report*.

33. National Institute of Standards and Technology (NIST). (2018). *Cybersecurity Framework*.

34. ENISA. (2020). *Public-Private Partnerships in Cybersecurity*.

35. Gartner. (2021). *Emerging Technologies in Cybersecurity*.

36. Mosca, M., & Piani, M. (2019). Quantum Computing and Post-Quantum Cryptography. *IEEE Security & Privacy*.

37. 5G Americas. (2019). *Security Considerations for 5G*.

38. SolarWinds. (2020). *Incident Analysis*.

39. Council of Europe. (2001). *Convention on Cybercrime*.

40. World Bank. (2017). *Building Cybersecurity Capacity*.

41. ENISA. (2020). *Public-Private Partnerships in Cybersecurity*.

42. Gartner. (2021). *Emerging Technologies in Cybersecurity*.

43. Cybersecurity and Infrastructure Security Agency (CISA). (2021). *Public Awareness Campaigns*.

44. Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., & Savage, S. (2013). Measuring the Cost of Cybercrime. *Workshop on the Economics of Information Security*.

45. Bradshaw, S., & Howard, P. N. (2019). The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation. *Computational Propaganda Research Project*.

46. Brenner, S. W. (2010). *Cybercrime: Criminal Threats from Cyberspace*. Praeger.

47. Case, T., & Marczak, B. (2016). Analysis of the Cyberattack on the Ukrainian Power Grid.

SANS ICS Security.

48. Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, 30(8), 719–731.
49. Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)*.
50. European Parliament. (2016). *General Data Protection Regulation (GDPR)*.
51. European Union Agency for Cybersecurity (ENISA). (2022). *Threat Landscape Report*.
52. Gartner. (2021). *Emerging Technologies in Cybersecurity*.
53. Healey, J. (2018). *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Cyber Conflict Studies Association.
54. Hong, J. (2012). The State of Phishing Attacks. *Communications of the ACM*, 55(1), 74–81.
55. ITU. (2018). *Global Cybersecurity Index*.
56. ITU. (2021). *Global Cybersecurity Agenda*.
57. Kshetri, N. (2017). Cybercrime and Cybersecurity in Developing Economies. *IT Professional*, 19(2), 11–14.
58. Kurbalija, J. (2017). *An Introduction to Internet Governance*. DiploFoundation.
59. Libicki, M. C. (2007). *Cyberdeterrence and Cyberwar*. RAND Corporation.
60. McAfee. (2018). *Economic Impact of Cybercrime*. Center for Strategic and International Studies.
61. Mitnick, K. D., & Simon, W. L. (2011). *The Art of Intrusion*. Wiley.
62. Mosca, M., & Piani, M. (2019). Quantum Computing and Post-Quantum Cryptography. *IEEE Security & Privacy*.
63. National Institute of Standards and Technology (NIST). (2018). *Cybersecurity Framework*.
64. Office of the Director of National Intelligence. (2020). *Annual Threat Assessment*.
65. PwC. (2017). *Global Economic Crime and Fraud Survey*.
66. Segal, A. (2016). *The Hacked World Order*. PublicAffairs.
67. Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.
68. SolarWinds. (2020). *Incident Analysis*.
69. Symantec Corporation. (2019). *Internet Security Threat Report*.
70. UN Office on Drugs and Crime. (2013). *Comprehensive Study on Cybercrime*.
71. UN Office on Drugs and Crime. (2018). *Cybercrime and Cybersecurity*.
72. US Department of Homeland Security. (2016). *Critical Infrastructure Cybersecurity*.
73. Verizon. (2018). *Data Breach Investigations Report*.
74. World Bank. (2017). *Building Cybersecurity Capacity*