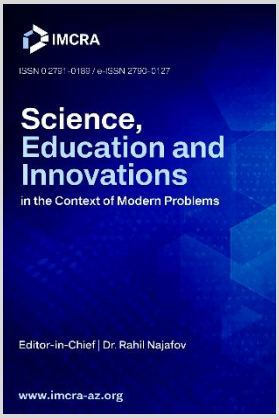

Science, Education and Innovations in the Context of Modern Problems
Issue 2, Vol. 9, 2026

RESEARCH ARTICLE

Transformations of Cybercrimes in the Context of Globalization: Patterns and Developments

Mounir Lomri
Doctor
Department of Law, Faculty of Law and Political Science, Mohamed Boudiaf University of M'sila
Algeria
E-mail: mounir.lomri@univ-msila.dz ; https:..orcid.org.0009-0008-5003-4627

Djagham Mohamed
Professor
Ecole normale superieure de BOU SAADA
Algeria
E-mail: djagham.mohamed@ens-bousaada.dz ; https:..orcid.org.0000-0003-4141-8369

Zouzou Zouleikha
Doctor
University of Biskra Algeria
Algeria
E-mail: Zouleikha.zouzou @ univ-biskra.dz; Orcid: https:..orcid.org.0009-0005-9093-0037

Issue web link https://imcra-az.org/archive/392-science-education-and-innovations-in-the-context-of-modern-problems-issue-2-vol-9-2026.html

Keywords Globalization; Cybercrime; Cybersecurity; Digital Transformation; Transnational Crime; Cyber Threat Intelligence; Critical Infrastructure Protection; Artificial Intelligence in Cybersecurity; Dark Web Economy; International Cyber Law.

Abstract

In the era of accelerated globalization and rapid digital transformation, cybercrime has evolved into a complex, transnational phenomenon that poses significant threats to individuals, institutions, and state infrastructures. This study provides a comprehensive and multidimensional analysis of the transformations of cybercrime within the context of globalization, focusing on emerging patterns, technological drivers, and future trajectories. Drawing upon interdisciplinary theoretical frameworks and contemporary empirical insights, the research examines how global interconnectedness, the expansion of digital economies, and the proliferation of advanced technologies—such as artificial intelligence, big data analytics, and encryption systems—have fundamentally reshaped both the scale and sophistication of cybercriminal activities. The study adopts an analytical-descriptive approach to explore three core dimensions: (1) the structural relationship between globalization and the evolution of cybercrime; (2) the emergence of new cybercrime patterns, including cyber espionage, attacks on critical infrastructure, and financially motivated cyber operations; and (3) the dynamic interplay between offensive cyber capabilities and defensive cybersecurity strategies. The findings reveal that globalization acts as a dual-force mechanism, simultaneously facilitating the diffusion of cybercrime tools and enhancing global cooperation in cybersecurity governance. Moreover, the research highlights the growing challenges associated with jurisdictional fragmentation, legal inconsistencies, and the increasing use of anonymization technologies that hinder effective law enforcement. The paper concludes that addressing the evolving landscape of cybercrime requires an integrated and forward-looking approach that combines adaptive legal frameworks, strengthened international collaboration, technological innovation in cybersecurity systems, and enhanced digital awareness. These findings contribute to the broader discourse on global security and digital governance, offering strategic insights for policymakers, legal scholars, and cybersecurity practitioners seeking to mitigate risks in an increasingly interconnected world.

Citation
Mounir L; Djagham M; Zouzou Z. (2026). Transformations of Cybercrimes in the Context of Globalization: Patterns and Developments. *Science, Education and Innovations in the Context of Modern Problems*, 9(2), 1-12. https://doi.org/10.56334/sei/9.2.104

Received: 01.04.2025	Accepted: 11.11.2025	Published: 22.02.2026 (available online)

Introduction:

With the accelerating pace of globalization and digital transformation, the world has witnessed unprecedented developments in the fields of technology and communications, leading to the emergence of advanced forms of cybercrimes targeting individuals, institutions, and even countries on a wide scale. These crimes are no longer limited to traditional methods such as electronic breaches and data theft but have extended to include more complex activities such as financial fraud, targeted cyberattacks, and even the exploitation of artificial intelligence technologies to carry out sophisticated crimes that are difficult to detect.

Amid this rapid landscape, it has become necessary to analyze and understand the radical transformations that have occurred in the nature of cybercrimes, not only in terms of the methods used or the targets aimed at but also regarding the profound effects that digital globalization has had on the spread of these crimes and the manner of their execution. The enhancement of global digital interconnectedness has created an intertwined cyber environment that facilitates the commission of crimes across national borders.

Globalization has contributed to fundamental transformations in emerging cybercrimes, as modern technologies such as artificial intelligence, big data analytics, and advanced encryption techniques are used not only to enhance cybersecurity but also to develop more sophisticated offensive methods. For example, cybercriminals now exploit technology to carry out complex financial frauds, cyberattacks targeting national infrastructure, and even hacking electoral systems and influencing public opinion through social media platforms.

Moreover, globalization has facilitated the spread of cybercrime by making the necessary tools more easily accessible, as malware or cyberattack services can be purchased via the dark web, enabling even non-professionals to conduct cyberattacks with capabilities that were previously limited to specialists. Additionally, the expansion of the digital economy and increased reliance on electronic systems in all fields have made financial institutions, government systems, and even individuals more vulnerable to targeting by organized crime networks that exploit technological advancements to achieve illicit gains.

This paper aims to analyze the patterns of cybercrime in the context of globalization, through three main axes:

1. Globalization and digital transformations and their impact on cybercrimes

2. Emerging patterns of cybercrime in the age of globalization

3. The evolution of cybercrime in the context of globalization

1.Globalization and digital transformations and their impact on cybercrimes

Technological progress has contributed to the rise in cybercrime rates, which have been exacerbated by the widespread effects of globalization. This development has led to the emergence of advanced methods that are exploited to carry out complex cyberattacks, taking advantage of digital openness and the expansion in the use of the Internet and modern technologies.

Literature Review

The rapid expansion of globalization and digital transformation has significantly reshaped the conceptual and operational landscape of crime, particularly in cyberspace. Existing literature consistently emphasizes that cybercrime is no longer a localized or technologically limited phenomenon but rather a complex, transnational issue deeply embedded within global socio-economic and political systems. Early theoretical contributions, such as those of Anthony Giddens, conceptualize globalization as the intensification of worldwide social relations, a process that inherently facilitates cross-border interactions, including illicit digital activities. This perspective provides a foundational framework for understanding how cybercrime has evolved alongside global interconnectedness.

A substantial body of research highlights the role of technological advancement as a primary driver of cybercrime proliferation. Scholars argue that the widespread adoption of information and communication technologies (ICTs), coupled with the expansion of the internet and digital economies, has created unprecedented opportunities for cybercriminal activities (Brenner, 2010). The emergence of sophisticated tools such as artificial intelligence, machine learning, and big data analytics has further transformed the nature of cyber threats, enabling attackers to conduct highly targeted and automated operations.

These developments have led to the emergence of advanced cybercrime typologies, including ransomware attacks, phishing schemes, cyber espionage, and large-scale data breaches.

In parallel, research has increasingly focused on the transnational dimension of cybercrime. According to contemporary studies, cybercrime operates beyond traditional geographical boundaries, often involving multiple jurisdictions in its execution and impact. This transnationality complicates legal enforcement and regulatory coordination, as national legal systems differ significantly in their definitions, enforcement mechanisms, and penalties related to cyber offenses (Ledingham & Mills, 2015). The absence of harmonized international legal frameworks creates regulatory gaps that cybercriminals exploit, thereby exacerbating the global spread of cyber threats.

Another critical strand of literature examines the relationship between globalization and the accessibility of cybercrime tools. The development of underground digital economies, particularly through dark web platforms, has democratized access to cybercrime-as-a-service models. Studies indicate that individuals with limited technical expertise can now engage in cybercriminal activities by purchasing ready-made malware, stolen data, or hacking services (Piscitello, 2017). This shift has lowered the barriers to entry for cybercrime and contributed to its rapid expansion across different social and economic contexts.

Furthermore, scholars have explored the increasing targeting of critical infrastructure by cybercriminals. Research shows that sectors such as healthcare, finance, energy, and transportation have become prime targets due to their reliance on interconnected digital systems and the high value of the data they manage. Cyberattacks on these sectors not only result in economic losses but also pose significant risks to national security and public safety (Boutalaa & Boukoro, 2022). The COVID-19 pandemic, in particular, highlighted the vulnerability of healthcare systems to cyber threats, reinforcing the urgency of strengthening cybersecurity resilience.

The literature also underscores the growing importance of cyber espionage in the context of globalization. Cyber espionage has evolved into a strategic tool used by both state and non-state actors to obtain sensitive political, economic, and military information. As noted in recent studies, advancements in digital technologies have enhanced the capacity for covert surveillance, data extraction, and information manipulation, thereby intensifying geopolitical tensions and security challenges in the digital age (Kalaa, 2022). This evolution reflects a broader shift toward the militarization of cyberspace as a domain of strategic competition.

In response to these escalating threats, a growing body of research focuses on cybersecurity strategies and governance mechanisms. Scholars emphasize the importance of adopting a multi-layered approach that integrates technological innovation, legal reforms, and international cooperation. Advanced cybersecurity measures, including encryption technologies, artificial intelligence-based threat detection systems, and real-time monitoring tools, are increasingly recognized as essential components of effective defense strategies. At the same time, international initiatives, such as the Budapest Convention on Cybercrime, aim to enhance cooperation among states, although their effectiveness remains limited due to uneven adoption and implementation.

Despite these advancements, significant gaps persist in the literature. One of the primary challenges lies in addressing the dynamic and rapidly evolving nature of cybercrime, which often outpaces legal and institutional responses. Additionally, the dual-use nature of emerging technologies—serving both defensive and offensive purposes—introduces new ethical and regulatory dilemmas. Scholars increasingly call for interdisciplinary research that integrates legal, technological, sociological, and economic perspectives to better understand and mitigate cyber risks in a globalized digital environment.

In summary, the existing literature provides a comprehensive foundation for understanding cybercrime as a multifaceted and evolving phenomenon shaped by globalization and technological innovation. However, the complexity of cyber threats and the limitations of current governance frameworks highlight the need for more integrated, adaptive, and globally coordinated approaches to cybersecurity.

1.1. Defining the conceptual framework of globalization and its development

Many think that globalization is primarily linked to economics or international economic research, but it also includes social, political, and cultural dimensions. An in-depth examination of globalization's nature shows it to be a complicated and layered idea, similar to numerous terms in the humanities that do not have a universally accepted definition. (Al-Khalayleh, 2018, p. 251).

Globalization refers to the increasing integration of societies, economies, and cultures worldwide, driven by technological advancements and cross-border economic and communication flows. Anthony Giddens defined it as "the intensification of social relations on a global scale, leading to the interconnectedness of distant societies in such a way that local events are affected by global events and vice versa."(Giddens, 1990, p. 64) Sadiq Jalal Azim defined it as an era of profound capitalist transformation of strategies collectively, under the hegemony, leadership and control of the central countries, under the dominance of a global system of unequal exchange (Weiss, 1998, p. 56). The International Conference on Culture, held in Cairo in November 2000, whose first theme was “Culture between Globalization and National Specificities,” stated that globalization is a historical process that extends deep into time on the one hand, and on the other hand, it is considered the ideology of the new world order (Salami & Sayhi, 2018, p. 14).

Globalization has a long history; it is not a recent phenomenon that emerged in the last few years, but rather has witnessed significant developments throughout the ages. However, the term became widely used after the end of the Cold War and the collapse of the Soviet system, becoming a fundamental concept in contemporary ideology. The scientific and technological revolution has contributed to the strengthening of globalization, particularly through the tremendous development of communication methods, such as the internet, satellites, and international information networks, which have accelerated the flow of information and facilitated communication across the globe (Abu Azza, 2022, p. 11). If we trace the historical origins of globalization, we can divide it into the following stages.:

***Formation phase:** This stage is considered the embryonic stage of globalization, as it arose as a historical phenomenon linked to the movement of conquests and expansion. (Al-Khudairi, 2005, p. 27).

***Birth stage:** This phase began with Canadian journalist Marshall McLuhan's formulation of the concept of the global village in his 1970 book, "War and Peace in the Global Village". It continued until the fall of the Berlin Wall in 1989 and the collapse of the Soviet Union in 1991, events that marked a major turning point in establishing globalization as a global phenomenon.

***Growth and expansion phase:** This phase began with the collapse of the Soviet Union and the declaration of what became known as the New International Order based on American exceptionalism, a concept introduced by former US President George H.W. Bush.This stage was characterized by the intertwining of economic, political, cultural, and social aspects, making the world more open and interconnected. The development of modern communication technologies accelerated interaction between individuals and societies to an instantaneous level, effectively eliminating geographical and temporal barriers (Robertson, 1998, p. 294). In this stage, information technology, the internet, and their advanced technologies became the cornerstones of rampant globalization, as the global market for information technology expanded significantly, reaching a peak in its development. Undoubtedly, some of these changes paved the way for the emergence of a global society.

1.2. The relationship between globalization and the rapid development of cybercrimes

The acceleration of globalization has led to the expansion of the digital space and the spread of modern technology, contributing to the emergence of new forms of cybercrime. While globalization has facilitated free global trade, it has also served the interests of crime and criminals. Thus, the concept of crime has benefited from the development of rapid communication and its sophisticated tools, increasing its spread across borders (Muqaddadi, 2000, p. 54). This relationship can be illustrated through the following points.:

1.2.1. Globalization as a catalyst for the development of cybercrime

Technological advancements in information technology have contributed, in various ways and through diverse methods, both complex and simple, to the evolution of crime at all social, economic, cultural, and political levels. The widespread adoption of digital technology has led to the emergence of new forms of crime, such as cybercrime, which includes hacking, digital fraud, data theft, and cyber espionage (Sharqi & Jabbar, 2015, p. 179). Furthermore, social media and artificial intelligence technologies have facilitated the manipulation of information and the dissemination of fake news, impacting social and political stability in many countries.

On the economic front, technological development has provided criminals with advanced means to launder money, evade taxes, and infiltrate banking systems, exploiting security gaps in the digital infrastructure of financial institutions. On the cultural front, technology has helped spread illegal content, such as pirated materials, immoral content, and incitement to violence, leading to new legal and ethical challenges for governments and societies.

From a political standpoint, cyberattacks on state infrastructure and cyber piracy targeting strategic objectives have become tools used in conflicts between states and groups, further complicating cybersecurity at the international level. (Wall, 2007)

Furthermore, the dark web has provided a suitable environment for the growth of cybercriminal activity. The dark web encompasses all websites not indexed by search engines. Some of these deep web sites are unconventional marketplaces offering a disturbing array of products and services. Here, you can buy or broker the purchase of illegal drugs, weapons, counterfeit goods, stolen credit cards, and hacked data.digital currenciesOr malware and national identity cards or passports. You can contract with digital or criminal services, starting with spam campaigns.(Spam) to distributed denial-of-service attacks. Even beginners can purchase ebooks explaining how to attack websites, steal identities, or otherwise profit from illicit activities. (Piscitello, 2017)

1.2.2. The impact of globalization on the spread of cybercrime across borders

Cybercrime is not confined to a specific geographical location. A criminal in one country can target victims in others without physically traveling. Modern crime is often transnational, as cybercrimes committed in one country have repercussions in another, with a third country benefiting. For example, computer gangs threaten to destroy the systems of financial institutions unless they are paid large sums of money or funds are transferred from one bank account to another. They rely on speed of execution via phone or keyboard, remotely, secretly, and without violence or evidence, making them attractive for investment and money laundering.(Al-Rawashdeh & Rabhi, 2017, p. 240) Cybercrime is considered a transnational crime, or

transnational organized crime, referring to criminal activities that transcend the borders of a single country and are carried out through coordination among multinational criminal groups. These crimes encompass a wide range of illicit activities.

Tracking cybercriminals is also a major challenge for security authorities, as criminals exploit sophisticated technologies to conceal their identity and complicate tracking and geographical location. Among these technologies are virtual private networks (VPNs).(VPN) to encrypt traffic and hide Internet Protocol (IP) addresses gives criminals the ability to carry out their activities without revealing their real geographical locations. In addition, these factors combined complicate law enforcement efforts, as identifying the perpetrators requires intensive efforts that include international cooperation and big data analysis to uncover suspicious patterns (Brenner, 2010). However, the difference in laws and efforts to combat cybercrime from one country to another hinders effective cooperation in pursuing cybercriminals.

Table 1. Evolution of Cybercrime Patterns in the Context of Globalization

Dimension	Traditional Cybercrime (Pre-Globalization Phase)	Contemporary Cybercrime (Globalization Era)	Key Transformation Drivers
Geographical Scope	Localized or nationally confined	Highly transnational and borderless	Global digital connectivity; internet penetration
Actors Involved	Individual hackers or small groups	Organized cybercriminal networks; state and non-state actors	Globalization of criminal networks; dark web ecosystems
Technical Complexity	Basic hacking, viruses, simple fraud	Advanced malware, AI-driven attacks, ransomware, cyber espionage	Artificial intelligence; big data; automation technologies
Target Profile	Individuals and small businesses	Critical infrastructure, governments, multinational corporations	Digitalization of essential sectors; data centralization
Tools and Platforms	Standalone software; limited tools	Cybercrime-as-a-Service (CaaS); dark web marketplaces	Accessibility of hacking tools; underground economies
Financial Impact	Relatively low and localized losses	Massive global financial damage and systemic risks	Expansion of digital economy; financial system integration
Detection and Attribution	Easier to trace and identify	Highly anonymized and difficult to attribute	Encryption technologies; VPNs; anonymization tools
Legal Frameworks	National laws with limited scope	Fragmented international legal responses	Lack of harmonized global cyber laws
Operational Speed	Slow and manual execution	Real-time, automated, and scalable attacks	High-speed networks; cloud computing

Table 2. Integrated Global Cybercrime Dynamics Model (IGCDM): Components and Relationships

Model Component	Key Variables	Functional Role	Impact on Cybercrime Dynamics
Globalization Drivers (Independent Variable)	Cross-border data flows; digital economy expansion; global connectivity	Structural enabler	Expands cybercrime reach and facilitates transnational operations
Technological Enablers (Mediating Variable)	AI, machine learning, encryption, blockchain, IoT	Capability amplifier	Increases sophistication, automation, and scalability of cyberattacks
Cybercrime Patterns (Dependent Variable)	Cyber espionage; ransomware; financial fraud; infrastructure attacks	Outcome variable	Reflects evolving forms and intensity of cybercrime
Regulatory Frameworks (Moderating Variable)	National laws; international agreements; enforcement mechanisms	Risk regulator	Weak frameworks increase cybercrime; strong governance mitigates risks
Cybersecurity Measures (Moderating Variable)	Firewalls; encryption systems; AI-based detection; awareness programs	Defensive mechanism	Reduces vulnerability and enhances system resilience
Dark Web Ecosystem (Intervening Variable)	CaaS platforms; illicit marketplaces; anonymization tools	Operational facilitator	Lowers entry barriers and accelerates cybercrime diffusion

International Cooperation (Control Variable)	Information sharing; joint investigations; treaties	Coordination mechanism	Enhances response effectiveness and reduces jurisdictional gaps

Cybercrime legislation is a necessary element in addressing the growing digital threats, but the disparity in national laws poses a significant challenge to their effective implementation. Countries establish their own regulations to combat cybercrime, and these laws often differ substantially, leading to legal loopholes that criminals may exploit. In addition, many of these laws do not take into account the transnational nature of cybercrime, making it difficult to coordinate legal efforts at the international level. ((Ledingham & Mills, 2015.)

Countries have different definitions of what constitutes cybercrime, which can lead to confusion and conflicts when dealing with cross-border cybercrime (Daraji & Jadidi, 2023, p. 1408). These legal differences negatively affect judicial cooperation between countries, which contributes to the expansion of cybercrime. Some governments may hesitate to extradite cybercriminals or exchange information due to the incompatibility of legal systems. For example, some countries impose strict penalties for cybercrime, while others lack sufficient legislation or clear legal procedures to combat these crimes. Furthermore, some international agreements, such as the Budapest Convention on Cybercrime, have not gained universal acceptance, which reduces their effectiveness in dealing with cross-border cases.

2. Emerging patterns of cybercrime in the age of globalization

Emerging patterns of cybercrime in the age of globalization include a variety of cyberattacks that exploit technological development and digital openness.

2.1. Cyberattacks on the digital infrastructure of countries and institutions

Infrastructure comprises the strategic objectives and vital facilities of any nation, and if targeted, it paralyzes the state and limits its ability to perform its essential functions. (Kamel, 2010, p. 2)

In this regard, reports from specialized international agencies indicate an increase in the number of cyberattacks targeting countries' strategic infrastructure, particularly energy, communications, transportation, financial systems, and biochemical industries, especially the healthcare sector during the COVID-19 pandemic.

The world's healthcare infrastructure, whether in times of peace or during armed conflict, and especially during pandemics, is vulnerable to cyberattacks. These attacks aim to disrupt computer systems, medical supply chains, and medical equipment, threatening to halt healthcare services and posing a serious risk to the lives of patients and healthcare workers. Such attacks also disrupt the distribution of essential supplies, exacerbating health crises and negatively impacting the response of medical systems to disasters. (Boutalaa & Boukoro, 2022, p. 331)

Furthermore, e-commerce and the financial services sector are essential components of a nation's critical infrastructure, given the vast amounts of sensitive and critical data they handle. Therefore, these sectors face the risk of technology misuse, which can disrupt services, undermine security and trust, and threaten financial stability at both the national and global levels. World Bank reports on settlement confirm these challenges, identifying the financial sector as the second most targeted by cyberattacks after the healthcare sector (Boutalaa & Boukoro, 2022, p. 333). For its part, the International Monetary Fund, based on studies conducted by the World Bank in 2012, indicated that the cost of cyberattacks targeting the financial sector in 81 countries worldwide is estimated at approximately 9% of global banks' net income (Ismail, 2019, p. 2).

In addition to the health and financial sectors, the energy sector has also not been spared from cyberattacks. This sector is not exempt from the risks of cyberattacks, whether for civilian or military use. Such attacks can cause severe damage, threatening civilian lives and impacting the environment, as well as disrupting related infrastructure. The reactor has witnessed...David Besse, a nuclear power plant in Ohio, suffered a cyberattack in 2013 that targeted its electronic networks, leading to the penetration and disruption of its control systems, and almost caused a nuclear disaster had it not been for the activation of the protection system that shut down the reactor automatically, according to what US officials stated. (Boutalaa & Bokoro, 2022, p. 334)

Cyberattacks on the transportation sector pose a growing threat. This sector relies on smart, internet-connected systems, such as traffic management systems, trains, and aircraft, making it an attractive target for cyberattacks. These attacks can disrupt transportation, steal or destroy passenger data, and even cause serious accidents. Ransomware attacks are among the most prominent threats facing the sector. Ransomware targets traffic control and automation systems in public transportation. With the increasing reliance on Internet of Things (IoT) technologies, advanced security measures to protect the sector's infrastructure have become essential.

The danger is amplified in armed conflicts, where transportation networks are targeted to pave the way for a military offensive, as happened before the 2015 Russian-Ukrainian confrontation. Cyberattacks may also be used as a weapon alongside traditional armed attacks. The events in Estonia in May 2007 remain a prime example, where the country suffered a large-

scale cyberattack that brought its vital sectors to a near standstill, including the official websites of the Prime Minister's office and Parliament (Butlaja & Bokoro, 2022, p. 335).

The 2.2. Cyber hacking and espionage crimes.

In light of the digital revolution, the rapid development of information technology, and the advancements brought about by globalization, the internet has become an indispensable part of our daily lives, leading to radical changes across various sectors. However, this development has been accompanied by numerous challenges, most notably cybercrime, particularly cyber espionage, which targets both individuals and organizations.

With the advancement of science and technology, cyber espionage methods have become more sophisticated and complex, posing a clear threat, especially with the increasing reliance on the internet for data management (Kalaa, 2022, p. 295). As these methods spread and evolved, new criminal patterns began to emerge on this network. (Rassaa, 2012, p. 10)

Cyber espionage consists of deliberate attempts to infiltrate the computer systems and websites of a hostile or adversary state with the aim of stealing confidential information (Mansour, 2019, p. 106). This type of espionage aims to collect vast amounts of data about military, political, security, economic, and industrial systems and secrets that rely primarily on modern communication and technological systems within countries.

Cyber espionage negatively impacts information security and communication systems, increasing the likelihood of sensitive information and secrets being leaked to other countries. It's important to note that cyber intelligence isn't limited to the official role of states and governments; it also extends to individuals who contribute to the production and dissemination of information, creating a vast database encompassing political and economic files across international borders. Intelligence agencies in various countries seek to collect, analyze, and utilize this information to serve their strategic interests.(Kalaa, 2022, p. 297)

Therefore, the developments brought about by globalization have led to an evolution in many crimes, including cyber espionage, which involves hacking websites and web pages on the internet with the aim of spying on or eavesdropping on their data and information, whether textual, audio, or visual, which may be of interest to the beneficiaries of the espionage, whether economic, commercial, political, or security-related..

These crimes also include sending emails to internet users containing software files capable of automatically transmitting information stored on the user's device, including text, audio, or video files. Furthermore, this software can transmit any data related to the user, such as their website browsing history, the data they enter (like username and password), and the search terms they use on global search engines. These crimes also include using specialized software to hack into internet-connected computers in order to spy on their contents..(Bouchoucha & Selmani, 2023, p. 53)

In addition to the above, the development of various technologies and the role of globalization in the modern era have led to a more comprehensive approach to espionage, extending beyond military and warfare domains to encompass economic, political, technological, and even social dimensions. While military espionage remains one of the most dangerous forms, the nature of the targeted information has changed significantly compared to the past. Military secrets are no longer limited to troop numbers and conventional weaponry, but now encompass advanced defense technologies, cyber warfare strategies, and modern intelligence systems. (Bouchoucha & Selmani, 2023, p. 53)

Technological advancements, particularly in the realm of the internet, have enhanced espionage capabilities, making it easier to target individuals, governments, and institutions, both national and international. The primary objectives of these modern intelligence activities fall into three main areas: the military, the political, and the economic, thus increasing the challenges associated with protecting strategic data and information..(Al-Alfi, 2013, p. 16).

3.The evolution of cybercrime in the context of globalization

With the continuous evolution of technology, cyber threats are expected to become increasingly complex in the coming years. Cybersecurity experts believe the future may hold unprecedented challenges.

3.1. The evolution of cyberattack methods

Among the most prominent technologies that have witnessed remarkable development under the influence of globalization are those used to perpetrate cybercrimes and launch cyberattacks. The digital revolution and rapid technological advancements have contributed to the emergence of sophisticated tools and methods exploited for illicit purposes, such as cyber intrusions, phishing attacks, malware, and cyber espionage, posing a growing threat to individuals, institutions, and nations alike. The evolution of these technologies has become a significant challenge, and some of the most prominent of these technologies include the following:

Malicious software: Malware is one of the most commonly used tools in cyberattacks. It consists of malicious programs designed to gain unauthorized access to computer systems, corrupt data, or disrupt critical infrastructure. Trojan horses are among the most common types.(Trojans), which disguise themselves as legitimate programs but perform malicious operations when run, and spyware, which collects confidential user information without their knowledge, in addition to viruses, which spread from file to file and cause damage to data and the operating system.

Ransomware: Ransomware is considered one of the most dangerous types of malware, as it encrypts the victim's data and prevents access to it until a ransom is paid to the attackers for its release. These programs use advanced encryption techniques, making it extremely difficult to decrypt them without paying the ransom. A well-known example of such an attack is the ransomware attack."WannaCry" which swept through thousands of systems around the world in 2017 by exploiting vulnerabilities in the Windows operating system.

***artificial intelligence:** Artificial intelligence is a powerful tool that can be exploited to enhance cyberattacks, as it can be used to create more sophisticated and intelligent malware capable of evading traditional security mechanisms. For example, machine learning techniques can be used to create such malware. Machine learning can be used to identify and exploit system weaknesses with unprecedented speed. AI-powered attacks can also target critical infrastructure, such as power grids and transportation systems, further increasing the risk.

Quantum computing attacks: With advancements in quantum computing, experts have begun warning of its potential to break traditional encryption systems. Quantum computers possess an unparalleled ability to perform calculations at tremendous speeds compared to conventional computers. This technology could render current encryption systems ineffective, necessitating the development of quantum-resistant encryption methods to protect sensitive data.(Symantec, 2021).

3.2. The development of methods for responding to and protecting cyber threats.

The evolution of cyberattack methods has not been unidirectional; it has been matched by a remarkable development in methods for confronting and countering these growing threats. Governments and security institutions have recognized the importance of strengthening their cybersecurity capabilities, leading them to adopt advanced technologies based on artificial intelligence and machine learning to analyze data and detect suspicious activity before an attack occurs. Sophisticated protection systems have also been developed, including smart firewalls, advanced antivirus software, and encryption technologies to ensure data confidentiality and integrity.

Furthermore, legislation and laws related to cybercrime have witnessed significant development to keep pace with technological advancements. Stringent laws have been enacted obligating companies and institutions to adhere to rigorous security standards and defining their responsibilities in the event of security breaches. Awareness campaigns and training have also played a crucial role in fostering a cybersecurity culture among individuals, helping to reduce security vulnerabilities that attackers could exploit.

Among the most prominent technologies that have developed in the field of combating cybercrime, we mention the following:

Firewall: A firewall is one of the most important digital security tools, preventing unauthorized access to private networks and thus contributing to the security of internet-based control and transmission equipment. Its importance lies in providing effective protection for networks that rely on multi-party broadcasting technologies, such as audio-visual equipment and video conferencing, enabling users to interact securely via audio and video without being vulnerable to hacking or intrusion. One example of such technology is software.Mphone, which is used for internet communication, may be vulnerable to surveillance attacks, making firewalls a necessity to protect communications and secure data.

Firewalls offer several advantages, most notably protecting the network and information from potential threats, while also enabling user monitoring and detection of any unauthorized access attempts. They log all activities and messages passing through the network, ensuring accurate data tracking and documentation of data traffic, thus enhancing digital security and reducing the likelihood of hacking or manipulation.. (Ben Haj Ali Faiza, 2019, p. 69).

***Evolution of encryption technologies:** Encryption technologies are a cornerstone of cybersecurity, playing a pivotal role in protecting data as it travels across networks, whether public or private. These technologies rely on converting information into complex codes that can only be read or understood by authorized parties, thus forming an effective barrier against hacking, espionage, and unauthorized use.

With rapid technological advancements, encryption techniques have undergone significant development to keep pace with escalating cyber threats. More sophisticated encryption algorithms, such as curve-based encryption and post-quantum encryption, have been developed to provide higher levels of security against advanced cyberattacks, particularly given the future risks posed by quantum computing. Encryption has also become an essential component of modern applications, from securing online communications, such as encrypted messaging apps, to protecting financial transactions and sensitive data in large organizations, thus enhancing information security in the digital age.

***systemInsurance in digital communications** Encryption protocols are among the most important methods used to protect data as it travels across the internet. They encrypt all communication between browsers and servers, reducing the chances of sensitive data falling into the hands of unauthorized parties. This protocol works by encrypting information as it is transmitted over the network, preventing any third party from accessing or manipulating it, thus enhancing user security and privacy. These protocols are primarily used to secure website logins, banking transactions, and e-commerce, as users need to ensure their personal and financial information is safe from hacking or phishing.

Furthermore, the security protocol gives users confidence in digital transactions, ensuring that transmitted information reaches only the intended recipient, whether it be an e-commerce merchant, a financial institution, or any other trusted entity. This system relies on advanced technologies such as the protocol.SSL.TLS, which is used to ensure data security through encryption, authentication, and integrity, has been shown in studies to increase customer trust and reduce the likelihood of electronic fraud by up to 70%. Therefore, investing in digital security systems is a pressing need in the modern era to ensure the safety of transactions and protect user data (Johnson, 2019).

Findings

The findings of this study reveal that cybercrime in the era of globalization has undergone a profound structural transformation, characterized by increased complexity, transnationality, and technological sophistication. First, globalization has significantly expanded the operational environment of cybercriminals by eliminating geographical constraints and facilitating instantaneous digital communication. This has enabled cybercrime to evolve from isolated incidents into highly organized, network-based activities operating across multiple jurisdictions.

Second, the analysis demonstrates that technological advancements—particularly in artificial intelligence, big data analytics, and encryption technologies—have played a dual role. On one hand, these technologies enhance cybersecurity capabilities; on the other, they are increasingly exploited by cybercriminals to develop more adaptive, automated, and difficult-to-detect attack strategies. The emergence of AI-driven malware, ransomware ecosystems, and advanced phishing techniques illustrates the growing asymmetry between offensive and defensive cyber capabilities.

Third, the study identifies a clear shift in the primary targets of cybercrime. While early cybercrimes largely focused on individuals, contemporary attacks increasingly target critical infrastructures, including financial systems, healthcare networks, energy grids, and governmental institutions. This shift reflects both the higher economic value of such targets and their strategic importance in national and global security contexts.

Furthermore, the findings highlight the growing significance of the dark web as an enabling ecosystem for cybercrime. The availability of cybercrime-as-a-service (CaaS) platforms has lowered the technical barriers to entry, allowing non-expert actors to engage in sophisticated cyberattacks. This democratization of cybercrime tools has contributed to the exponential growth in the number and diversity of cyber threats.

Another key finding concerns the limitations of existing legal and regulatory frameworks. The transnational nature of cybercrime, combined with inconsistencies in national legislation and enforcement mechanisms, creates significant challenges for international cooperation. Despite efforts to harmonize legal responses through international agreements, gaps in jurisdiction, extradition policies, and data-sharing practices continue to hinder effective cybercrime mitigation.

Finally, the study underscores the necessity of adopting a holistic and integrated cybersecurity approach. Effective responses to cyber threats require not only technological solutions but also coordinated policy frameworks, international collaboration, and increased awareness among individuals and institutions. The findings suggest that cybersecurity resilience is fundamentally dependent on the alignment of technological innovation, legal governance, and global cooperation mechanisms.

Model Framework

To conceptualize the relationship between globalization, technological advancement, and cybercrime dynamics, this study proposes an Integrated Global Cybercrime Dynamics Model (IGCDM). The model is designed to explain how structural global factors interact with technological and institutional variables to influence the evolution of cybercrime.

1. Core Components of the Model

The framework consists of four interrelated dimensions:

(1) Globalization Drivers

- Cross-border digital connectivity
- Expansion of the digital economy
- Global information flows and network integration

These drivers create an open and interconnected digital environment that facilitates both legitimate and illicit activities.

(2) Technological Enablers

- Artificial Intelligence (AI)
- Big Data Analytics
- Encryption and anonymization technologies (e.g., VPNs, blockchain)

These technologies act as amplifiers, enhancing both cyber offense (e.g., automated attacks) and cyber defense (e.g., predictive threat detection).

(3) Cybercrime Patterns (Dependent Variable)

- Cyber espionage
- Financial cybercrime (fraud, ransomware)
- Attacks on critical infrastructure
- Cybercrime-as-a-service (CaaS)

This dimension represents the evolving forms and operational strategies of cybercrime.

(4) Regulatory and Defensive Mechanisms

- National cybersecurity policies
- International legal frameworks
- Cybersecurity technologies and awareness systems

These mechanisms aim to mitigate cyber threats but are often constrained by fragmentation and lack of coordination.

2. Conceptual Relationships

The model assumes the following relationships:

- H1: Globalization positively influences the expansion and transnationalization of cybercrime.
- H2: Technological advancement mediates the relationship between globalization and cybercrime sophistication.
- H3: Weak or fragmented regulatory frameworks significantly increase cybercrime risks.
- H4: Strong cybersecurity governance and international cooperation reduce the impact and spread of cybercrime.

3. Model Interpretation

The IGCDM framework suggests that cybercrime is not merely a technological issue but a systemic outcome of global structural transformations. Globalization acts as the primary catalyst, while technological innovation accelerates both the scale and complexity of cyber threats. Regulatory systems function as moderating variables; their effectiveness determines whether cyber risks are contained or amplified.

The model further highlights a feedback loop mechanism, where increasing cyber threats stimulate advancements in cybersecurity technologies and legal reforms, which in turn influence future cybercrime strategies. This dynamic interaction underscores the need for adaptive and forward-looking cybersecurity policies.

4. Practical Implications of the Model

- Supports policymakers in designing integrated cyber governance strategies
- Assists cybersecurity professionals in understanding emerging threat patterns
- Provides a foundation for empirical testing using quantitative or mixed-method approaches
- Enhances interdisciplinary research linking law, technology, and global studies

Conclusion

The technological growth observed globally, particularly during the twentieth century and the start of the twenty-first century, has helped boost globalization and its extensive spread. Communication among people and organizations has become simpler and quicker, resulting in major changes in several economic and social areas. However, this digital advancement has come with difficulties, as it has seen a clear increase in cybercrimes that have grown more complicated and organized than ever before. These crimes now target not just individuals but also large organizations and governments, endangering cybersecurity and threatening the stability of the global economy. Looking at future trends, new technologies such as artificial intelligence and strong encryption are important for improving data security and safeguarding digital systems. However, these advanced technologies can also be a double-edged sword, as cybercriminals might misuse them to create more advanced strategies for carrying out cyberattacks. Therefore, tackling this rising threat needs a comprehensive approach that merges flexible legislation development, boosting international teamwork in cybersecurity, applying advanced technology solutions, and increasing digital awareness to create a safer and more sustainable online environment amid ongoing technological changes.

Ethical Considerations

This study was conducted in full compliance with internationally recognized research ethics standards and principles. The research does not involve human participants, personal data, or experimental procedures requiring institutional ethical approval. All sources used in this study have been properly cited and acknowledged in accordance with academic integrity and anti-plagiarism standards. The authors confirm adherence to the ethical guidelines recommended by the Committee on Publication Ethics, ensuring transparency, honesty, and accountability throughout the research and publication process.

Conflict of Interest

The authors declare that there are no financial, professional, or personal conflicts of interest that could have influenced the research, authorship, or publication of this article. The study was conducted independently, and all interpretations and conclusions are solely those of the authors.

Funding Statement

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors. The authors confirm that the study was conducted without external financial support.

Author Contributions

All authors contributed significantly to the conception, design, and development of this study.

- Mounir Lomri: Conceptualization, methodology, writing – original draft, supervision.
- Djagham Mohamed: Theoretical framework development, critical review, validation.
- Zouzou Zouleikha: Literature review, data analysis, editing and proofreading.

All authors have read and approved the final version of the manuscript and agree to be accountable for all aspects of the work.

Data Availability Statement

No primary datasets were generated or analyzed during this study. The research is based on secondary data, theoretical analysis, and previously published sources, all of which are properly cited within the manuscript.

Acknowledgements

The authors express their sincere gratitude to their respective academic institutions for providing the necessary intellectual environment and support for conducting this research. They also acknowledge the contributions of scholars and researchers whose work has informed and enriched this study.

Consent for Publication

All authors have reviewed the final manuscript and provide their full consent for its publication. The manuscript has not been previously published and is not under consideration for publication elsewhere.

Plagiarism and Originality Statement

The authors affirm that this manuscript is an original work and has not been copied, plagiarized, or published previously in any form or language. All sources and references have been appropriately cited. The manuscript complies with international standards of academic integrity and originality.

AI Use Statement

The authors declare that no artificial intelligence (AI) tools were used in the generation of the research content, data analysis, or core academic writing of this manuscript. Any minor language editing tools, if used, did not affect the intellectual content or scientific conclusions of the study.

Publisher's Note

The publisher remains neutral with regard to jurisdictional claims in published maps, institutional affiliations, and geopolitical representations.

References

1. Al-Khalaileh, A. B. A. (2018). Dimensions of Cultural Globalization on Arab Identity in the Age of Unipolarity. Heritage Journal, 8(1), 251.
2. Giddens, A. (1990). The consequences of modernity. Stanford University Press.
3. Weiss, S. (1998). Arab Time and the Global Future. Arab Future Publishing House.
4. My greetings, ASaihi, A. (2018). Threats facing Arab culture in light of the challenges of cultural globalization: Reality and challenges. Algerian Journal of Research and Studies, 1(3), 14.
5. Abu Azza, A. R. (2022). The Concept of Globalization: Its Historical Origins and Stages of DevelopmentAl-Asala Magazine, (2), 11.
6. Al-Khudairi, M. (2005)Globalization and Contemporary Society. Arab Thought House.
7. Robertson, R. (1998)Globalization: Social, Theoretical, and Cultural World (translated by M. Maud & A. Amin). Supreme Council for Culture and Publishing.
8. Muqaddadi, M. (2000)Globalization: Many necks, one sword. Dar Al-Far Publishing.
9. Al-Rawashdeh, ARabhi, A. (2017). Cybercrimes in the Era of Globalization: An Analytical Study of Structure and Countermeasures. Journal of the Department of Legal and Political Research and Studies, (3), 240.
10. Brenner, S. W. (2010). Cybercrime: Criminal threats from cyberspace. ABC-CLIO.
11. Ledingham, R., & Mills, R. (2015). A preliminary study of autism and cybercrime in the context of international law enforcement. Advances in Autism, 1(1).
12. Dragi, ShJadidi, D. D. R. (2023). The threat of cross-border cybercrime: international challenges and strategies to counter it. Academic Journal of Legal and Political Research, 7(2), 1408.
13. Kamel, M. A. R. (2010, December). Threats to Critical Information Infrastructure. In the 15th Annual Conference: Water and Water Resources Crisis Management, Potential Scenarios and Constructive Balanced Strategies(Volume 2). Ain Shams University.
14. Butalaa, andBokoro, M. (2022). Cyberattacks on Critical Infrastructure: A Study in Light of Public International Law. Journal of Human Rights and Public Freedoms, 7(2), 331.
15. Ismail, M. (2019). Cybersecurity in the Banking SectorPublic Policy Brief, Arab Monetary Fund, (4), 2.
16. Kala, Sh. (2022). Cybersecurity and the challenges of espionage and cyber intrusions against states via cyberspace,Journal of Law and Humanities, 15(1), 295–297.
17. Rassaa, F. (2012). Criminal Protection of Information on the Internet (Master's Thesis in Public Law). Faculty of Law and Political Science, Abou Bekr Belkaid University – Tlemcen, Algeria.
18. Mansour, Sh. A. and. (2019Fifth-generation warfare: "insider attacks" on the international stage. Arab Publishing and Distribution.
19. Bushusha, SSalmani, H. (2023). Cyber Espionage and Methods of Combating It. Journal of Humanities and Social Sciences, 16(1), 53.
20. Al-Alfi, M. M. (2013). Legislation to Combat Cyberterrorism Crimes: Substantive Provisions and Patterns. Working paper presented at the Scientific Symposium on Arab and International Laws in Combating Terrorism, Riyadh, Saudi Arabia, p. 16.
21. Symantec. (2021). Malware threats and protection.Symantec
22. Johnson, M. (2019). Secure transactions and online trust: The role of encryption. Cambridge University Press.