Cybercrime in Spain and Türkiye: Comparative Analysis of Threats, Legislation and Proposals for Improvement

Adrián Nicolas Marchal González

Prof., Antonio de Nebrija University, Department of Security and Defense, Madrid, SPAIN,
e-mail: amarchal@nebrija.es (ORCID: 0000-0001-8647-1214)

ARTICLE INFO

Research Article

Received Date: 17 November 2024

Accepted Date: 16 Decemder 2024

Citation: González, A.N.M. (2024). Cybercrime in Spain and Türkiye: Comparative Analysis of Threats, Legislation and Proposals for Improvement. Almanac Diplomatique, 1(1). 88-102

Abstract

In an interconnected world, cybercrime represents a growing threat that transcends borders, impacting economies, critical infrastructures, and social trust in the digital environment. This study provides a comparative analysis of Spain and Türkiye, two nations with distinct socio-political contexts but shared vulnerabilities to cyberattacks. The article examines key threats such as phishing and ransomware, their impact on critical infrastructures, and the national strategies and legislative frameworks adopted to address them.

Spain stands out for its adherence to the Budapest Convention and the implementation of inclusive policies that foster public-private collaboration, while Türkiye prioritizes the development of national capacities and technological sovereignty. Despite progress, both countries face significant challenges, including barriers to international cooperation, legal gaps concerning emerging technologies, and limitations in specialized resources.

The article highlights the need for coordinated, adaptive, and sustainable approaches, emphasizing cybersecurity education and public-private collaboration as essential pillars. Finally, it proposes strategies to improve international collaboration and strengthen regulatory frameworks, contributing to a more effective response to global cyber threats.

Keywords: Cybercrime, Türkiye, Spain.

Introduction

In an increasingly interconnected world, cybercrime emerges as one of the greatest threats to global security. This phenomenon not only compromises the stability of digital infrastructures, but also profoundly affects national economies, institutions and citizens. According to recent estimates, the economic impact of cybercrime amounted to €7 trillion in 2022, with projections to reach €10.5 trillion by 2025, surpassing even entire national economies.

Cybercriminals have found digitalisation fertile ground to innovate their attack methods, from traditional techniques such as phishing and ransomware to sophisticated social engineering attacks (Limón, 2024).

Cybercrime does not recognise borders, and both Spain and Türkiye have faced particular challenges in this area. In Spain, according to the Cybercrime Report 2023, cybercrime accounted for 19.2% of all criminal offences, with fraud being the most common type. Türkiye, strategically located between Europe and Asia, faces a complex landscape where cybercrime is intertwined with transnational dynamics, such as data trafficking and the proliferation of organised cybercrime.

This comparative analysis seeks to identify patterns, differences and opportunities for cooperation between the two countries, considering legislative particularities, technical challenges and operational approaches.

The impact of cybercrime is multidimensional:

Economic: The return on investment in cybercrime activities is estimated to be over 1,400%, making it a more profitable “business” than drug trafficking.

Social: From identity theft to online harassment, individual victims suffer not only material but also psychological losses.

Critical Infrastructure: Attacks targeting sectors such as transport, energy or banking can cripple entire economies.

Both countries have taken significant steps to combat cybercrime. In Spain, the reform of the Penal Code and the ratification of the Budapest Convention have strengthened the regulatory framework. In Türkiye , the integration of EU-inspired measures has been key to harmonizing its legislative response. (Leal Ruiz, 2021)

At the international level, bodies such as INTERPOL and EUROPOL have been instrumental in coordinating transnational operations and developing information exchange platforms.

Cybercrime is a global challenge that requires a coordinated, innovative and sustainable approach. This comparative analysis between Spain and Türkiye seeks not only to identify areas for improvement, but also to lay the foundations for closer and more effective cooperation in the fight against this threat.

In an era where digital transformation has become a cornerstone of global economic and social development, cybercrime represents an escalating threat that transcends borders, legal systems, and technological safeguards. The research problem addressed in this study is the divergence in national strategies and legislative responses to cybercrime between Spain and Türkiye, two countries with distinct socio-political contexts but shared vulnerabilities to cyber threats. Despite the global nature of cybercrime, these differences create barriers to effective collaboration, leaving critical gaps in the global cybersecurity landscape.

Spain and Türkiye have experienced a significant rise in cybercrime incidents in recent years, ranging from ransomware attacks targeting critical infrastructure to sophisticated phishing campaigns aimed at defrauding individuals and businesses. According to recent estimates, cybercrime in Spain accounts for 19.2% of all recorded criminal activity, while Türkiye faces complex challenges due to its geopolitical position, which facilitates transnational cybercrime networks. These trends underline the urgent need for an in-depth comparative analysis of how each country perceives, legislates, and operationally addresses cybercrime.

This study is important for several reasons. First, it provides a systematic examination of the unique and shared challenges faced by Spain and Türkiye, offering insights into the effectiveness of their current legal and institutional frameworks. Second, the research highlights opportunities for harmonization and collaboration, particularly in areas where international cooperation is crucial, such as the exchange of intelligence and the prosecution of cross-border cybercriminals. Finally, this study fills a critical gap in the literature by focusing on two countries that, despite their regional and cultural differences, are pivotal to Europe and Asia's cybersecurity landscapes.

By identifying areas of strength and weakness in the respective approaches of Spain and Türkiye this study aims to contribute to the development of more robust and cooperative frameworks for combating cybercrime. The findings are not only relevant for policymakers and law enforcement agencies in both countries but also for the broader international community seeking to mitigate the ever-evolving threats posed by cybercrime.

This article is structured into six main sections to provide a comprehensive comparative analysis of cybercrime threats, legislation, and proposals for improvement in Spain and Türkiye. First, the phenomenon of cybercrime is defined and conceptualized, detailing its scope, typology, and fundamental characteristics. The second section examines the most common cyber threats faced by both countries, with a particular focus on their socio-economic impact and associated risks.

The third section explores the national legal and regulatory frameworks, analyzing the key laws, policies, and cybersecurity strategies implemented in Spain and Türkiye, and highlighting the institutions responsible for their enforcement. The fourth section identifies the main challenges in combating cybercrime, including technical, legal, and operational obstacles that hinder the investigation and prosecution of these crimes.

In the fifth section, the study presents proposals for improvement aimed at strengthening international cooperation, promoting legislative harmonization, and enhancing technical and human capacities to prevent and mitigate cyber threats. Finally, the conclusions synthesize the key findings and reflect on the implications of the comparative analysis for designing more effective strategies against cybercrime.

This study contributes to the existing body of literature by undertaking a comparative analysis of cybercrime in Spain and Türkiye, two nations with distinct socio-political landscapes and cybersecurity challenges. While prior research has predominantly focused on broader regional or global frameworks, this article provides a detailed examination of the specific threats, legislative measures, and institutional responses in these countries. By identifying common patterns and divergences, the study offers valuable insights into the effectiveness of current strategies and the potential for cross-border cooperation.

Moreover, this research goes beyond theoretical analysis by integrating data from practical case studies, official reports, and legislative texts. In doing so, it bridges the gap between academic discourse and policy implementation, providing actionable recommendations for strengthening national and international approaches to cybercrime. This work also emphasizes the role of emerging technologies and evolving cyber threats, which remain underexplored in existing literature.

By addressing these gaps, the study aims to advance scholarly understanding of cybercrime while offering pragmatic solutions to policymakers, practitioners, and international organizations working to mitigate this complex and evolving threat.

Conceptualisation of Cybercrime

Definition and scope of cybercrime.

Cybercrime has been a topic of growing interest in recent years, both in Spain and Türkiye. However, before addressing the characteristics and types of cybercrime, it is essential to understand the concept of cybercrime itself. (Coronado Contreras, 2021).

The definition of cybercrime varies depending on the source, but in general it refers to the commission of crimes using information and communication technologies (ICT) to obtain benefit or cause harm. In the Spanish context, the Penal Code does not have an explicit definition of cybercrime, but it is considered to be a generic term that encompasses several types of digital crimes.

Cybercrime is closely related to other concepts such as cybercrime, cybersecurity and personal data protection. Cybercrime refers to the commission of crimes using ICT, while cybersecurity refers to the measures taken to prevent and detect cybercrime. The protection of personal data is a crucial aspect in the fight against cybercrime, as many digital crimes involve the illegal collection and use of personal information.

This phenomenon has evolved significantly over the last decades. In the 1990s, cybercrime was mainly focused on breaching systems and spreading viruses. However, with the advancement of technology and the popularisation of the Internet, cybercrime has evolved to include new types of crime, such as phishing, identity theft and malware dissemination. (López Gorostidi, 2022).

Cybercrime can be classified into several types, depending on its nature and target. Some of the most common types of cybercrime are computer system breaches, which refers to the unauthorized infiltration of computer systems to gain access to confidential information; phishing, which is the sending of fraudulent messages that appear to come from a legitimate source with the aim of obtaining personal or financial information; and identity theft, which refers to the illegal collection and use of personal information to commit crimes.

Cybercrime can have serious consequences for victims, including loss of personal information, identity theft, reputational damage and financial loss. In addition, cybercrime can also affect the wider economy, as it can cause significant losses for businesses and individuals.

The fight against cybercrime is a complex challenge that requires the collaboration of multiple actors, including governments, businesses and international organisations. (Almenar Pineda, 2018). Some of the most important challenges in the fight against cybercrime include the lack of effective regulations to prevent and punish cybercrime, the difficulty to detect and investigate cybercrime due to the complexity of the technologies used, and the need to improve international cooperation to share information and coordinate efforts in the fight against cybercrime.

In short, conceptualising cybercrime involves understanding the concept of cybercrime itself, its characteristics and types, and the challenges society faces in combating this crime (Dimitrakos, 2023). Developing a thorough understanding of cybercrime is essential to effectively address this problem and to protect individuals and the economy at large.

Socio-Economic Impact and Associated Risks

The socio-economic impact and risks associated with cybercrime are significant and vary depending on several factors, such as the type of attack, the industry affected and the level of preparedness of the private and public sector. Cybercrime can have devastating economic consequences, ranging from financial losses and reputational damage to loss of trust in government institutions and systems.

Risks associated with cybercrime include loss of sensitive information, identity theft, extortion and data hijacking. In addition, cybercrime can affect different sectors, such as banking, technology companies, governments and financial institutions. (Conal, 2023).

It is important to stress that cybercrime affects not only businesses and individuals, but also society at large. The loss of trust in institutions and governance systems can have serious political and social consequences. It is therefore essential that governments, businesses and individuals work together to prevent and combat cybercrime.

Preventing cybercrime requires a comprehensive strategy that includes cyber security training, implementation of robust security measures and collaboration between government agencies and businesses. In addition, it is important to develop a clear regulatory framework to address the risks associated with cybercrime.

The socio-economic impact and risks associated with cybercrime are significant and require a coordinated and effective response from governments, businesses and individuals.

Major Common Cyber Threats

The main common cyber threats include phishing attacks, malware, ransomware, hacks and identity theft.

Other common types of cyber threats include denial of service (DoS) attacks, which can cause an interruption in service to a website or network; cross-site scripting (XSS) attacks, which can allow an attacker to execute malicious code on a website; and SQL injection attacks, which can allow an attacker to access an application's database.

It is important to be aware of these common cyber threats and take measures to protect against them, such as using up-to-date antivirus software, avoiding opening suspicious emails and not accessing unsafe websites. However, we will be looking at the main threats that have impacted Spain and Türkiye in recent years (Dunn Cavelty, 2024).

Malware and Ransomware

Malware is malicious software designed to damage or steal data from a computer system. It can be transmitted through emails, file downloads, visits to infected websites or through the use of infected USB devices.

Types of malware include: (i) Adware, which displays unsolicited advertisements to the user and may collect information about the user's browsing habits. (ii) Spyware, which may collect personal information from the user without their knowledge or consent. (iii) Ransomware, which encrypts the user's files and demands payment in exchange for the decryption key.

It is important to note that malware can be transmitted accidentally by opening a suspicious email or downloading an infected file (Pfleeger, 2024). Therefore, it is essential to keep all software up to date and avoid clicking on suspicious links or opening suspicious files.

Ransomware is a particularly aggressive form of malware that has become a growing threat to Internet users. It works by encrypting the user's files and demanding a payment in exchange for the decryption key. Ransomware is often difficult to remove and can cause irreparable damage to the user's data.

Examples of ransomware include PETYA, which was reported by Heise Security, and others such as WannaCry, NotPetya and LockBit. (Del Villar, 2021). These attacks have had a significant impact on organisations and businesses around the world, highlighting the need to take measures to protect against this type of threat.

Phishing and Electronic Fraud

Phishing is a form of electronic fraud that involves sending fake emails or text messages that appear to come from a trusted source, with the aim of obtaining personal or financial information from the recipient. Attackers may use techniques such as phishing to make the user believe that the message is from a bank, payment company or government authority. (Rey Huidobro, 2013).

These messages often contain malicious links or malware-infected attachments, which can cause damage to the user's computer systems. The ultimate goal is to gain unauthorized access to bank accounts, credit cards or sensitive personal information.

In 2023, both in Spain and Türkiye, thousands of incidents related to phishing and electronic fraud were recorded in different areas of the public and private sector. These incidents have had a significant impact on organisations and businesses around the world, highlighting the need to take measures to protect against this type of threat.

Cybercriminals often use techniques such as spoofing to make the user believe that the message comes from a trusted source. For example, they may send an email that appears to come from the CEO (CEO scam) or manager of a company, with the aim of gaining access to confidential information or conducting unauthorized financial transactions.

It is essential to be cautious when receiving suspicious emails or text messages and not to click on malicious links or open infected attachments. It is also important to keep antivirus software up to date and use security tools to protect against this type of threat.

Attacks on Critical Infrastructure

Critical infrastructure attacks are a type of cyberattack that aims to compromise the security and stability of systems and networks that are critical to economies and society at large. These infrastructures may include power plants, drinking water systems, public transport, hospitals and other essential services (Walters, 2021).

Attackers can use techniques such as ransomware, phishing and phishing to gain access to these systems and networks and cause damage. The objectives of these attacks can be varied, ranging from financial gain to causing physical or psychological harm to individuals. (López Gorostidi, 2022).

In 2023, several incidents related to attacks on critical infrastructure were reported in different parts of the world. For example, in one Latin American country, a group of hackers used ransomware to attack the public transport network of a major city, causing a total shutdown of the service.

In another case, an attacker used phishing to gain access to a hospital's systems and steal patients' personal information. These incidents have highlighted the need for organisations and businesses to take steps to protect themselves against this type of threat and ensure the security and stability of their critical infrastructures.

To prevent these attacks, it is essential to implement robust security measures, such as firewalls, intrusion detection systems and up-to-date anti-virus software. In addition, it is important to conduct emergency drills and incident response exercises to ensure the ability to respond quickly in the event of an attack.

Cyber-terrorism and Cyber-espionage

Cyberterrorism and cyberespionage are concepts related to the use of information and communication technologies to commit acts of terrorism or espionage. Cyberterrorism refers to cyber attacks that aim to cause harm or terror in a society, while cyberespionage focuses on the collection of secret information without permission. (Madrid Parra, 2022).

Today, these concepts have become increasingly important due to the increased use of the internet and social media, which has facilitated communication and collaboration between individuals and groups. Terrorists and spies can use these platforms to spread hate messages, incite violence or gather sensitive information on potential targets (Kuan-Ching, 2019).

Governments and organisations have implemented measures to combat these types of threats, including the creation of cyber defence units and international collaboration to share information and best practices. However, cyberterrorism and cyberespionage remain major challenges in the digital age.

The criminal law punishes with penalties lower than those provided for the offence in question anyone who publicly disseminates messages or slogans suitable for inciting others to commit any of the offences defined in this article, which are aimed at or are suitable for favouring a climate of violence, hostility, hatred or discrimination against the aforementioned groups. The above penalties shall be imposed in their upper half when the acts have been carried out through a means of social communication, via the internet or through the use of information technology, in such a way that it is accessible to a large number of people.

Legal and Regulatory Framework in Spain

National legislation on cybercrime.

Spanish national legislation on cybercrime is contained in several laws and provisions that seek to protect the security and integrity of citizens in the digital environment. The main laws include Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights, which regulates the protection of personal data and establishes measures to prevent cybercrime.

Also relevant is Organic Law 11/1995 of 29 December 1995 on the Protection of National Security, which includes measures to prevent and repress terrorist activities online. Law 10/2019 of 4 April on National Cybersecurity establishes a regulatory framework for national cybersecurity and fosters collaboration between public and private actors. (Segura Serrano, 2023). Spanish legislation also specifically addresses aspects such as intellectual property online, the protection of minors in the digital environment and the prevention of money laundering through financial technologies. In addition, Spain has a regulatory framework governing civil liability for damages in cyberspace, which aims to protect citizens from potential legal vulnerabilities.

National cyber-security policies and strategies.

Spain’s National Cybersecurity Policy focuses on achieving a secure use of Information and Telecommunications Systems, strengthening the capacities for prevention, defense, detection and response to cyber-attacks. To achieve this objective, a policy is promoted that brings together and coordinates all institutions and agents with responsibility in this area. (López-Muñoz, 2020). An appropriate regulatory framework is developed to regulate the use of information and communication technologies (ICTs) and to ensure security in cyberspace. This policy aims to create a secure environment so that citizens, businesses and institutions can carry out their activities without risk.

Spain's cybersecurity strategy focuses on several fronts:

Prevention: The aim is to prevent cyber-attacks by implementing effective security measures, such as the protection of personal data and early detection of threats.

Defence: Capabilities are developed to defend against cyber-attacks, including incident response and recovery of affected systems.

Detection: Threat detection systems are implemented to identify and neutralise potential risks before attacks occur.

The response: Effective response procedures are established in the event of a cyber-attack, including the reporting of incidents to the competent authorities.

Spain's national cybersecurity policy is an ongoing effort to improve security in cyberspace and protect citizens' trust in the use of ICTs. It seeks to create a secure and trustworthy environment so that companies and institutions can carry out their activities without risk and citizens can enjoy the benefits of technology without exposure to risk. (Canals Ametller, 2021).

Responsible Bodies and Institutions

Spain's national cybersecurity policy aims to coordinate and bring together all institutions and agents with responsibility in this area. Below are some of the key bodies and institutions involved in the implementation of this policy.

The Ministry of the Interior is the body responsible for public security and the prevention of terrorism, including cybersecurity aspects. The Ministry of the Interior has the Central Cybercrime Unit, which is responsible for investigating and preventing cybercrime (Ministry of Interior, 2024).

The Ministry of Defence is another key body in the field, as it focuses on critical infrastructure protection and national defence. The Ministry of Defence has, among others, the Joint Cyberspace Command, which is in charge of cybersecurity and critical infrastructure protection.

The State Secretariat for Digitalisation and Artificial Intelligence is responsible for the implementation of the country's digital strategy, including aspects related to cybersecurity. The State Secretariat has the National Cyber Institute (INCIBE), which is responsible for promoting cyber awareness and the prevention of cybercrime (INCIBE, 2024).

The National Police is a key institution in the field, as it focuses on citizen security and crime prevention. The National Police has the Central Cybercrime Unit and the Computer Crime Investigation Brigade, which are responsible for investigating and preventing cybercrime.

The Spanish Data Protection Agency is responsible for the protection of personal data and privacy online. There is also the National Cryptologic Centre, which is responsible for promoting cyber awareness and the prevention of cybercrime.

In summary, Spain's national cybersecurity policy is coordinated by a number of key agencies and institutions, including the Ministry of the Interior, the Ministry of Defence, the Secretary of State for Digitalisation and Artificial Intelligence and the National Police. These institutions work together to implement effective measures to prevent cybercrime and protect online security. (Fontestád Portalés, 2020).

Legal and Regulatory Framework in Türkiye

National legislation on cybercrime.

Türkiye's national legislation on cybercrime is regulated by several laws and regulations. Law No. 6458, known as the "Cyberspace Law", is the main law governing cybersecurity in the country. This law establishes the basis for the protection of national security online and punishes cybercrime.

The law defines the concepts of cyberspace, personal data and digital identity, and establishes the responsibilities of internet service providers and network operators to ensure online security. It also regulates the collection and use of personal data online. Law no. 5651, known as the "Cybercrime Law", is another important law specifically sanctioning cybercrimes in Türkiye. This law defines and punishes the following conducts as cybercrimes: dissemination of false or misleading information, unauthorized access to computer systems, digital identity theft, and other forms of cybercrime.

Law no. 6238, known as the "Data Protection Law", is another law that relates to the protection of personal data in Türkiye. This law establishes the rules for the collection, use and protection of personal data, both online and offline.

Turkish cybercrime legislation is based on the Turkish Penal Code (TPC) and complementary laws that specifically address cybercrime. A detailed analysis of the requested aspects is presented below:

The CPT addresses cybercrime in a number of articles that criminalise conduct related to the misuse of computer systems:

Unlawful access to information systems (Article 243): Criminalises unauthorized access to information systems.

Alteration or destruction of data (Article 244): Penalises the modification, destruction or inhibition of data in computer systems.

Misuse of devices (Article 245): Punishes the production, sale or possession of devices designed to commit computer-related crime.

In addition, Law No. 5651 on the Regulation of Internet Publications and the Fight against Crimes Committed through Internet Publications complements the CPT by establishing responsibilities for online content and service providers.

National Cyber Security Policies and Strategies

Türkiye has developed a series of strategies and measures to strengthen its national cyber security, focusing on the protection of critical infrastructure, government institutions and private companies. These are detailed below:

In December 2020, Türkiye announced its 'National Cybersecurity Strategy and Action Plan 2020-2023', marking a milestone in its efforts to consolidate security in cyberspace. This plan is a continuation of previous strategies, such as 2013-2014 and 2016-2019, reflecting a steady evolution in the country's cybersecurity policy.

The 2020-2023 strategy is structured in eight chapters outlining key objectives:

Protection and strengthening of critical infrastructures: Recognising the importance of sectors such as energy, telecommunications and finance, measures are implemented to safeguard these systems from potential cyber-attacks.

National capacity building: The training of specialised professionals and the creation of own technologies are promoted in order to reduce dependence on foreign solutions.

Organic cybersecurity network: Effective coordination is sought between public and private entities, establishing channels of communication and collaboration for a rapid response to incidents.

Security of emerging technologies: Addresses challenges associated with the adoption of new technologies, such as artificial intelligence and the Internet of Things, ensuring their secure implementation.

Combating cybercrime: Law enforcement capabilities are strengthened to prevent, detect and prosecute criminal activities in cyberspace.

Development and support for national technologies: Research and development of local technological solutions is encouraged, fostering innovation and self-sufficiency in cybersecurity. Integration of cybersecurity into national security: Cybersecurity is recognised as an essential component of national security, integrating it into defense policies and strategies.

Advancing international cooperation: Collaboration with other countries and international organisations to address global cyber threats is promoted.

A central component of this strategy is the Turkish Cyber Incident Response Centre (TR-CERT), established in 2013. TR-CERT plays a crucial role in identifying and mitigating cyber threats, coordinating with sectoral teams and providing national incident response (TR-CERT, 2023). To safeguard its critical infrastructure and key entities, Türkiye has implemented a number of measures:

Cyber Incident Response Teams: It has become mandatory for public and private institutions managing critical infrastructure to form SOME teams. These teams operate under the coordination of TR-CERT and are in charge of monitoring, detecting and responding to cyber incidents, ensuring a proactive and coordinated defense. Development of National Technologies: The 2020-2023 strategy emphasises the importance of developing and supporting national technologies. This approach seeks to reduce dependence on foreign solutions, strengthening digital sovereignty and promoting local innovation in cybersecurity.

Specific Regulations for Critical Infrastructure: The Energy Market Regulatory Authority has issued guidelines that include asset and risk management, penetration testing and security audits, and compliance with standards such as ISO 27001 and 27019. These regulations seek to ensure that critical infrastructures, especially in the energy sector, maintain high levels of security and resilience against potential cyber threats. (Carli García, 2024).

These initiatives reflect Türkiye's commitment to strengthening its cyber security posture, protecting both government institutions and the private sector, and ensuring the resilience of its critical infrastructure in the face of growing threats in cyberspace.

Responsible Bodies and Institutions

In Türkiye, cybersecurity is managed through a complex institutional structure involving various government entities, law enforcement, academic institutions and the private sector. This comprehensive collaboration aims to protect the country's digital environment from cyber threats and ensure the resilience of its critical infrastructure.

The Ministry of Transport and Infrastructure plays a central role in the development of cybersecurity policies and regulations (Ministro of Transport and Infrastructure, 2020). The ministry is responsible for developing national strategies and action plans that strengthen the country's digital security. For example, it has implemented national cybersecurity action plans, such as the one covering the period 2016-2019, with the aim of establishing sound national cybersecurity, formulating and coordinating efficient and sustainable policies, and implementing those policies in practice. (ICEX, 2020).

Furthermore, the ministry has emphasised the importance of digitalisation and cybersecurity for Türkiye's economic development and sovereignty, highlighting the integration of advanced technologies and the strengthening of digital infrastructure as key to building a secure and prosperous nation (Dunn Cavelty, Cyber security politics : socio-technological transformations and political fragmentation, 2022).

Within the structure of the Ministry of Transport and Infrastructure is the Cyber Emergency Response Centre (TR-CERT), known in Turkish as Ulusal Siber Olaylara Müdahale Merkezi (Bravo, 2024). Established on 27 May 2013, TR-CERT is responsible for the analysis and mitigation of large-scale cyber threats, communicating information about malicious activity or potential vulnerabilities to cyber security incident response teams and the general public (Anon, 2022). Its mission includes the protection of government and citizen cyberspace, taking measures to safeguard both public and private critical infrastructures, such as energy production and distribution, water management and telecommunications institutions. TR-CERT also organises international cybersecurity exercises, such as "Cyber Shield 2019", which simulates common cyber attacks to improve response capabilities and foster international cooperation in cybersecurity.

The General Directorate of Security (Emniyet Genel Müdürlüğü) and the Gendarmerie play key roles in the fight against cybercrime. These institutions are responsible for investigating and controlling crime in the digital environment, tackling illicit activities such as cyber espionage, online fraud and other cybercrime. They work in coordination with other government agencies and international bodies to conduct effective investigations and law enforcement in cyberspace.

Türkiye's National Security Council also plays a significant role in defining digital defence strategies. This body, in collaboration with the Turkish Armed Forces, develops cyber defence policies and coordinates actions to protect the country from cyber threats that could compromise national security. The integration of cybersecurity into national security is a priority, and measures have been taken to strengthen cooperation between the different entities involved in digital defence. (Burak Daricili, 2021). The participation of private and academic entities is essential in Türkiye's national cybersecurity ecosystem. Universities and technology companies collaborate with the government in research and development initiatives, training of specialised personnel and creation of innovative solutions to address cyber challenges. For example, TR-CERT, in cooperation with the "ICTA Academy" (BTK Akademi), has provided various cybersecuri tytraining, ranging from web application security to computer forensics. In addition, TR-CERT offers hands-on training to cybersecurity enthusiasts in the "Fetih Cyber Drill Field". At the international level, Türkiye liaises with bodies such as the International Telecommunication Union (ITU) and the Cybersecurity Alliance for Mutual Progress (CAMP) to strengthen its cybersecurity posture. TR-CERT is a member of the Forum of Security Incident Response Teams (FIRST) and the Organisation of Islamic Cooperation Computer Emergency Response Team (OIC-CERT), which facilitates cooperation and information sharing with other countries in the fight against cyber threats.

In summary, Türkiye has developed a robust institutional structure to address cybersecurity challenges, involving multiple government entities, law enforcement, academia and the private sector (Kaschner, 2021). Effective coordination among these actors is essential to ensure the protection of the country's digital environment and to respond efficiently to emerging cyber threats.

Challenges in the Fight Against Cybercrime

Obstacles in the investigation and prosecution of cybercrime.

The investigation and prosecution of cybercrime present multiple challenges that complicate the work of law enforcement authorities. These obstacles are manifested both in Türkiye and globally, and range from technical complexities to legal and resource constraints.

Cybercriminals employ advanced technologies that make it difficult to identify and locate them. The use of strong cryptography makes it possible to encrypt communications and data, preventing authorities from accessing information crucial to investigations. Virtual private networks (VPNs) and the dark web provide anonymity and facilitate illicit activities without leaving obvious traces. For example, in Türkiye, cases have been detected where criminals use the dark web to sell stolen personal data, complicating their traceability due to the anonymity provided by this platform (Fahey, 2022).

The transnational nature of cybercrime poses significant challenges for coordination between countries. Legal differences and barriers to information sharing hinder international cooperation. An illustrative case is the WannaCry ransomware attack in 2017, which affected multiple countries, including Türkiye, and highlighted the need for closer collaboration between nations to address global cyberthreats. (Arrazola Ruiz, 2021). In Türkiye, law enforcement and cybersecurity agencies face limitations in human, technological and financial resources. The shortage of trained cybersecurity personnel and the lack of advanced technologies reduce the effectiveness of cybercrime prosecution. For example, the Turkish National Police has recognised the need for increased specialised training to effectively address cyber threats.

The acquisition, preservation and validity of digital evidence are critical aspects of investigations. Criminals employ techniques to erase traces and encrypt information, complicating the collection of evidence. In Türkiye, cases have been reported where the lack of adequate forensic tools has prevented the collection of sufficient evidence to prosecute those responsible for cybercrime. Collaboration with technology companies is essential, but is often met with resistance due to privacy and reputational concerns. In Türkiye, some companies have been reluctant to share data relevant to investigations, making it difficult to identify and prosecute cybercriminals. This lack of cooperation may be due to fear of affecting their customers' trust or facing legal repercussions. Users' lack of knowledge and caution contributes to the proliferation of cybercrime. In Türkiye, cybersecurity awareness campaigns have been limited, resulting in a population vulnerable to online scams and attacks. The absence of education on safe internet practices makes it easier for criminals to exploit these weaknesses.

In summary, the fight against cybercrime in Türkiye and globally faces multiple challenges that require a coordinated and multifaceted response. Strengthening international cooperation, updating legal frameworks, investing in resources and training, fostering public-private partnerships and raising social awareness are essential to effectively address these obstacles.

Legislative Adaptation to New Technologies

Cybercrime has emerged as one of the main threats in the digital age, forcing countries to adapt their legal frameworks to deal with crimes that transcend borders and evolve rapidly. Both Türkiye and Spain have undertaken legislative reforms to address these challenges, although they face significant obstacles in their implementation. Technological advances have challenged traditional regulatory frameworks, requiring constant updates to address new forms of crime. In Spain, the accession to the Budapest Convention in 2010 marked a milestone in the fight against cybercrime, establishing a legal basis for prosecuting cybercrime and facilitating international cooperation. (Jariego Ruiz, 2023).

Subsequently, in 2022, Spain signed the Second Additional Protocol to the Convention, focusing on enhanced cooperation and disclosure of electronic evidence. Türkiye, meanwhile, has shown a more restrictive approach in its digital legislation. In 2020, the Turkish government passed laws that increase control over digital platforms and restrict freedom of expression online, which has led to criticism from human rights organisations.

These measures, while seeking to combat cybercrime, have been questioned for their impact on fundamental rights. Despite legislative efforts, there remain areas where current laws do not adequately address emerging cybercrimes. The use of technologies such as artificial intelligence, blockchain and cryptocurrencies has introduced new forms of crime that challenge existing regulations. For example, the anonymity offered by cryptocurrencies makes it difficult to trace illicit transactions, while artificial intelligence can be used to perpetrate sophisticated attacks that are not covered by current laws. In addition, the emergence of the metaverse raises questions about jurisdiction and the applicability of traditional laws in virtual environments.

Rapid technological change often outpaces the ability of legislators to adapt legal standards. The legislative process, which includes debates, consultations and approvals, is often slower than the pace of technological innovation. This creates a time lag that cybercriminals can exploit, operating in unregulated areas or exploiting loopholes in the law. In addition, the lack of technology experts within legislative bodies can hinder the understanding and effective regulation of new technologies.

The implementation of new laws must balance the fight against cybercrime with the protection of fundamental rights such as privacy, freedom of expression and access to information. In Spain, the Organic Law on the Protection of Personal Data and Guarantee of Digital Rights seeks to protect citizens' privacy in the digital environment. However, in Türkiye , recent reforms have been criticised for restricting freedom of expression and increasing state surveillance, raising concerns about respect for human rights in the fight against cybercrime.

Conclusions

The impact of cybercrime is multidimensional, affecting not only the economy, with losses reaching billions of euros, but also critical infrastructures and social trust in the digital environment. Spain and Türkiye are particularly affected due to their strategic positions and the digitisation of their economies, although the types of threats and their prevalence vary between the two countries. Phishing attacks, ransomware and incidents targeting critical infrastructure stand out as the most damaging, underlining the sophistication of the methods used by cybercriminals.

From a legislative point of view, Spain and Türkiye have taken significant steps to strengthen their response capacity. Spain stands out for its accession to the Budapest Convention and its legal framework including the Organic Law on Personal Data Protection, while Türkiye has implemented laws such as the "Data Protection Law" and the "Cybercrime Law". In terms of strategies, both countries have developed action plans focused on prevention, detection, defense and response to cyberattacks. Spain has strengthened cooperation between public and private actors, while Türkiye has prioritised the development of national capabilities and the reduction of foreign technological dependence. These efforts reflect a growing understanding that cyber security must be integrated as an essential component of national security, although significant challenges remain in the effective implementation of these strategies.

International cooperation emerges as a critical pillar in the fight against cybercrime. Organisations such as INTERPOL, EUROPOL and CERTs in both Spain and Türkiye have played a central role in coordinating transnational efforts, although legal differences and limitations in information sharing continue to hinder the effectiveness of these collaborations. The increasing use of emerging technologies such as artificial intelligence and cryptocurrencies adds complexity, exposing legal and regulatory gaps that need to be urgently addressed. Finally, it is necessary to reinforce the need to advance cybersecurity education and awareness at both the individual and institutional levels. Training in secure practices and promoting a culture of cybersecurity are essential to mitigate vulnerabilities and strengthen resilience to attacks. It is also essential to foster more effective public-private collaboration and to ensure adequate resources are allocated to the investigation and prosecution of cybercrime.

This Spain-Türkiye analysis highlights both achievements and areas for improvement in the fight against cybercrime. Although each country faces unique challenges, the shared experience underlines the importance of a comprehensive, coordinated and adaptive approach to not only respond to current threats, but also to anticipate and prepare for emerging risks in the digital environment.

References

Almenar Pineda, F. (2018). *Ciberdelincuencia* . Porto: Jurúa.

Anon. (2022). *Cyber Security : Critical Infrastructure Protection.* Cham: Springer.

Arrazola Ruiz, S. (2021). La ciberdelincuencia como fenómeno jurídico. Su tratamiento procesal . *Revista Aequitas:*, 371-402.

Bravo, J. (30 de octubre de 2024). *DPL*. Retrieved from https://dplnews.com/infraestructura-tecnologica-y-ciberseguridad-fortalecen-la-soberania-digital/

Burak Daricili, A. (1 de enero de 2021). *AA*. Retrieved from https://www.aa.com.tr/es/mundo/turqu%C3%ADa-lleva-a-la-ciberseguridad-nacional-a-otro-nivel-/2098185

Canals Ametller, D. (2021). *Ciberseguridad : un nuevo reto para el Estado y los Gobiernos Locales.* Madrid: Wolters Kluwer.

Carli García, M. (23 de marzo de 2024). *CCI-ES*. Retrieved from https://www.cci-es.org/maps/turquia/

Conal, C. (2023). *Ciberseguridad y derecho penal.* Pamplona: Aranzadi.

Coronado Contreras, J. (2021). *Ciberterrorismo, ciberdelincuencia y cooperación internacional* . Madrid: Wolters Kluwer.

Del Villar, J. (8 de septiembre de 2021). *IDTY*. Retrieved from https://www.idty.com/es-la/5-de-los-mayores-ataques-de-ciberseguridad-en-los-ultimos-anos

Dimitrakos, T. (2023). *Collaborative approaches for cyber security in cyber-physical systems.* Switzerland: Springer.

Dunn Cavelty, M. (2022). *Cyber security politics : socio-technological transformations and political fragmentation.* Abingdon: Routledge.

Dunn Cavelty, M. (2024). *The politics of cyber-security.* New York: Routledge, Taylor & Francis Group.

Fahey, E. (2022). *The EU as a global digital actor : institutionalising global data protection, trade, and cybersecurity* . Oxford: Hart Publishing, Bloomsbury Publishing Plc.

Fontestád Portalés, L. (2020). Jurisdicción y competencia internacional en materia de ciberdelincuencia . *Tirant lo Blanch*, 235-334.

ICEX. (2020). *El mercado de la ciberseguridad en Turquía.* Ankara: ICEX España Exportacion e Inversiones.

INCIBE. (2024). *National Institute of Cybersecurity* . Retrieved from https://www.incibe.es/en

Infrastructure, M. o. (2020). *National Cybersecurity Strategy and Action Plan 2020-2023*. Retrieved from https://www.uab.gov.tr/

Interior, M. o. (2024). *Ministry of Interior. Central Cybercrime Unit*. Retrieved from https://www.interior.gob.es/opencms/en/inicio

Jariego Ruiz, E. (2023). Ciberdelincuencia : amenaza en la red y la oportunidad del Convenio de Budapest. *Diario La Ley*, 34-42.

Kaschner, H. (2021). *Cyber crisis management : the practical handbook on crisis management and crisis communication.* Wiesbaden: Springer Vieweg.

Kuan-Ching, L. (2019). *Advances in cyber security : principles, techniques, and applications.* Singapore: Springer.

Law 10/2019, of April 2, on National Cybersecurity. Official State Gazette, No. 79, April 2, 2019 Retrieved from https://www.boe.es/eli/es/l/2019/04/02/10

Law No. 5651 on the Regulation of Internet Publications and Combating Crimes Committed via Such Publications. (2007, May 23). Official Gazette of Turkey, No. 26530. Retrieved from https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5651.pdf

Law No. 6698 on the Protection of Personal Data. (2016, April 7). Official Gazette of Turkey, No. 29677. Retrieved from https://www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law

Leal Ruiz, R. (2021). *Ciberdelincuencia : Temas prácticos para su estudio .* A Coruña: Colex.

Limón, R. (2 de Junio de 2024). *El País*. Retrieved from https://elpais.com/tecnologia/2024-06-02/los-ciberataques-alcanzan-su-maximo-historico-no-hay-nadie-a-salvo.html

López Gorostidi, J. (2022). *Ciberdelincuencia : proporcionalidad y bienes jurídicos protegidos .* Granada: Comares.

López Gorostidi, J. (2022). Sobre el alcance de los fines de la pena en el fenómeno criminal de la ciberdelincuencia. *Revista chilena de derecho y tecnología*, 119-158.

López-Muñoz, J. (2020). *Cibercriminalidad e investigación tecnológica .* Madrid: Dykinson.

Madrid Parra, A. (2022). *Derecho digital y nuevas tecnologías.* Pamplona: Aranzadi.

Organic Law 3/2018, of December 5, on the Protection of Personal Data and the Guarantee of Digital Rights. Official State Gazette, No. 294, December 6, 2018, pp. 119788-119857 Retrieved from https://www.boe.es/eli/es/lo/2018/12/05/3

Pfleeger, C. P. (2024). *Security in computing.* Boston: Addison-Wesley Professional.

Rey Huidobro, L. F. (2013). La estafa informática relevancia penal del phishing. *La ley penal*, 50-62.

Segura Serrano, A. (2023). *El desafío de la ciberseguridad global : análisis desde el derecho internacional y europeo.* Valencia: Tirant lo Blanch.

Spanish Penal Code, consolidated text. Official State Gazette, No. 281, November 24, 1995 Retrieved from https://www.boe.es/eli/es/lo/1995/11/23/10/con

Turkish Penal Code (Law No. 5237), Articles 243-245. (2004, October 12). Official Gazette of Turkey, No. 25611. Retrieved from https://www.wipo.int/edocs/lexdocs/laws/en/tr/tr171en.pdf

TR-CERT. (2023). *Turkish Cyber Emergency Response Team*. Retrieved from https://www.usom.gov.tr/

Walters, R. (2021). *Cyber security, artificial intelligence, data protection & the law.* Singapore: Springer.

Almanac Diplomatique

2024

Almanac Diplomatique emerges as a distinguished blog and e-journal, meticulously devoted to the scholarly study and analysis of International Relations. This platform stands at the forefront of academic discourse, offering a profound exploration of diplomacy, public diplomacy, international law, and a spectrum of related disciplines that underpin the global geopolitical landscape.

www.almanacdiplomatique.com