Global Journal of Arts, Humanities and Social Sciences
Vol.13, No.2, pp.35-56, 2025
Print ISSN: 2052-6350(Print)
Online ISSN: 2052-6369(Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Cyber-crime and Cybersecurity Legislation in Europe and Albania: A State-of-the-Art Research

Dr. Arben Prifti
Faculty of Law, and Humanities "The Mediterranean University of Albania ", Albania

doi: https://doi.org/10.37745/gjahss.2013/vol13n23556 Published February 11, 2025

Citation: Prifti A. (2025) Cyber-crime and Cybersecurity Legislation in Europe and Albania: A State-of-the-Art Research, *Global Journal of Arts, Humanities and Social Sciences*, Vol.13, No.2, pp.35-56

Abstract: *The swift progression of information technologies, especially the Internet of Things (IoT), has significantly reshaped modern society. While IoT presents considerable advantages, it simultaneously introduces notable challenges, particularly concerning cybercrime, a form of criminal activity marked by extensive societal risks. This research paper investigates the development of cybercrime, emphasizing Albania's legislative alignment with European Union standards and practices. Through a historical, analytical, descriptive, and comparative methodology, the research outlines the present condition of cybercrime in Albania, in comparison with the European Union's policies and legal frameworks. Even though the country's endorsement of the Budapest Convention on Cybercrime and various cybersecurity efforts, the incidence of cybercrime continues to escalate, highlighting the necessity for improved national and international collaboration. The paper also examines the European Union's all-encompassing approach to cybersecurity, stressing the importance for member states to establish sturdy legal frameworks and cooperative mechanisms to effectively counter cyber threats. Furthermore, it assesses Albania's legislative actions against cybercrime, identifying potential areas for enhancement in capacity development and international cooperation. In conclusion, this study emphasizes the critical need for a united endeavor in the fight against cybercrime and the augmentation of cybersecurity across borders to protect both national and international interests.*

Keywords: cyber-crime, cyber-security, Internet of Things, cyber-attacks, National security cooperation

INTRODUCTION

Emerging information technologies, particularly the Internet of Things (ToI), have acquired significant relevance in contemporary society both in its advancements and its deviance (AlSalem et al.,2023). This progression influences not only the operations of governmental and private entities but also impacts individuals in their daily routines, both in personal and professional contexts. As with any novel technology accessible to a broad demographic, the ToI offers numerous advantages and benefits; however, it simultaneously introduces a range of challenges that were previously inconceivable. The exploitation of technology by delinquents and extreme deviants is termed 'cybercrime,' which is recognized as a category of crime characterized by a substantial social risk

(Philips et al.,2022). Fundamentally, it involves individuals engaging with a computer system, potentially manifesting as computer fraud, forgery, breaches of security systems, or any other forms that utilize a connected computer system as a medium. Cybercrimes are described as: "*Criminal activities directed against individuals or groups for financial gain, damaging the victim's reputation, or inflicting physical or psychological harm, either directly or indirectly, through the use of contemporary technology*" (Philips et al.,2022). By their nature, new technologies undergo continuous evolution, and consequently, the associated risks similarly transform. Confronted with the challenges posed by cybercrime, numerous nations endeavor to delineate their boundaries through filtering mechanisms and the establishment of electronic barriers (Adeyeri & Abroshan,2024). However, this recent variant of crime has transcended previous limitations regarding time and physical boundaries, affecting multiple state districts. Therefore, it is insufficient for a single state to implement preventive strategies against this issue. Collaboration between two or more states or allies is imperative to yield effective results in the prevention and mitigation of this phenomenon. The Council of Europe has made a significant contribution in this regard, serving as the preeminent institution in safeguarding the interests of member states through coordination and enhanced cooperation among them. The European Union has likewise played an important role in addressing this issue by employing community instruments (such as directives, decisions, and recommendations). Consequently, countries that aspire to join the EU are required to integrate the entire body of community legislation into their legal frameworks. One such country is Albania, which, in alignment with the adherence criteria established by the EU, is obligated to advance the development and execution of national legislation concerning the investigation, prosecution, adjudication, and international cooperation in the fight against cybercrime. The prevalence of cybercrime in Albania is escalating in various forms. Despite Albania's ratification of the "Budapest Convention on Cybercrime" and several cyber security agendas, there is a clear necessity for further legislative reforms in this domain in terms of national and international cooperation. The present article seeks to analyze the state-of-the-art of the current cyber-security and cyber-crime in Albania compared to the European Union both in terms of macro and micro development.

METHOD

In the current paper, several scientific methodologies were employed, which encompass the examination of the phenomenon of cybercrime considering its progression and emergence within an era characterized by significant technological advancement, particularly as viewed through the lens of both European and national legal regulations. The methods utilized in this research include historical, analytical, descriptive, and comparative methods, all which interconnect within the addressed topics. The *historical method* has been employed to illustrate the evolutionary trajectory of cybercrime, along with the progressive in several European countries and within the European Union and the alignment of Albanian domestic legislation with the acquis Communautaire pertinent to cybercrime. The *analytical method* is found on a thorough legal scrutiny of the provisions and actions of both Community and domestic law relating to cybercrime. The *descriptive approach* utilized seeks to ascertain the current state of cybercrime development and to delineate the stance of our nation towards this issue within the context of the international and European obligations undertaken, by providing an elaborate overview and comprehensive analysis of the European and domestic legal frameworks concerning cybercrime to identify the challenges faced in this domain, as well as the effective application of best practices within the Albanian context. *The comparative method* has been

employed to juxtapose the sanctions instituted by European legislation aimed at the prevention and combat of cybercrime with their practical implementation across various countries, as compared to the regulatory measures established by the Albanian legislator.

The European Union Policies in addressing Cybercrime and Cybersecurity

Cyber crisis represents a genuine systemic threat impacting all advanced societies, including the European Union (Boeke,2017). They pose risks to all socio-economic entities, including public administrations, resulting in considerable costs to the internal market (Admass et al.,2023). The adverse effects of escalating and increasingly sophisticated cyber threats extend beyond economic lines and may even jeopardize the safety of citizens. To combat these threats, the Union must adopt a unified vision and foster instruments that support the formation of a collective unit for cyberspace. The European Cybersecurity Authority (ENISA) emphasizes that attacks have become more sophisticated and impactful, driven by the continuous expansion of digital technologies, exacerbated by the Covid-19 pandemic and especially during the War in Ukraine, the shift toward interconnected and cloud-based infrastructures, and the utilization of emerging technologies such as artificial intelligence (see ENISA,2025). The initial action in the domain of cybersecurity at the European level was the European Commission's Communication on Network Security in 2001(see the EU Commission Communication,2001) which was implemented following the Budapest Convention on Cybercrime (see the Convention of Budapest,2001) established by the Council. The Commission noted that "*policy measures in this domain can hold a dual advantage: enhancing the internal market economically while simultaneously improving the legal framework*." Communication also emphasizes the necessity for a coordinated approach, not only at the European level but also globally. Since that time, the Union has leveraged policies, regulations, and financial resources to bolster its cyber resilience. Considering the increasing frequency of significant cyber-attacks and incidents, initiatives in this area have increased since 2013, accompanied by the adoption of initial national cybersecurity strategies by Member States. From its earliest communications, the Commission has consistently underscored the importance of harmonizing both substantive measures, which relate to the definition of offenses and security protocols, and procedural, thus organizational, measures among the various Member States to guarantee an adequate level of cybersecurity. In November 2009, the introduction of security protocols in electronic communications was proposed through Directive 2009/140/EC (see Directive 2009/140 EC), [no longer in force], which modifies the earlier Directive 2002/21/EC that governs electronic communications services and networks, emphasizing their security and integrity. Following this, on 7 February 2013, the European Union Cybersecurity Strategy was enacted to streamline the European cybersecurity framework, encouraging all Member States to establish specific national legislation aimed at preventing and addressing disruptions and attacks impacting telecommunications systems in Europe (see the EU Cybersecurity Strategy,2013). A few months later, on 12 September 2013, the European Parliament ratified Resolution No. 2013/2606 "*on the European Union Cybersecurity Strategy: An Open and Safe Cyberspace*" (see Resolution No.2013/2606). Furthermore, the 2018 EUCSS includes the Directive on Security of Network and Information Systems (NIS Directive) and a communication from the Commission that emphasizes the significance of collaboration between public and private sectors, acknowledging the strategic importance of such partnerships(see NIS Directive,2018).The 2013 European Union Cybersecurity Strategy (EUCSS 2013) employes a range of legislative measures, both binding and non-binding, designed to create an open, secure, and safeguarded cyberspace. The components of the strategy outline actions focused on the prevention of cybercrime, while simultaneously safeguarding

critical infrastructure and enhancing network security (see the EU Cybersecurity Strategy,2013). In 2017, the Commission indicated the necessity of establishing a European framework for addressing large-scale cybersecurity incidents and crises. It is essential to facilitate the rapid and accurate transmission of information from technical experts to policymakers, passing through the operational tires of policy officers and crisis managers: the primary aim is to respond in a coordinated fashion and assist Member States that are experiencing difficulties. Timely communication of the causes, effects, and potential countermeasures to a cyber crisis is crucial for reducing risks to citizens and minimizing potential economic harm to the Union's economy (see the EU Agenda,2025). Thus, the European cyber security framework aims to enable an efficient and coordinated response in alignment with the objectives outlined in the European Cybersecurity Strategy Agenda (see the EU Agenda,2025).

International Laws and Jurisdiction of Cyberspace: Rules and Regulations

ICT systems function as computerized systems and, as such, are "susceptible" in various respects. For instance, the software utilized may exhibit an inherent vulnerability at a technical level, allowing unauthorized access (breach) to confidential or governmental entities, thereby undermining the security of the data held or transmitted. In simpler terms, human error is a possibility; external agents may manipulate the operator to render access or data available without authorization (the *social engineering attack*). A quintessential illustration of this is phishing, characterized by the dispatch of emails from third parties that deceitfully compel the recipient to disclose sensitive information and access credentials for other systems. Occasionally, emails appear to originate from recognizable entities (*spear-phishing*), yet the credentials have been fabricated. All these methodologies are well-established and aim to appropriate sensitive information or to implant software (Trojan) within the computer system that can subsequently disseminate unauthorized information autonomously and render it permissible to the Deep Web. The European Agenda on Cybersecurity 2025 established that member countries hold authority over ICT infrastructures situated within their borders. Each State autonomously regulates its cyberspace (see the EU Agenda on Cybersecurity,2025). The report further stated that every State exercises sovereignty over its territory in alignment with international law, while considering the sovereignty of other States, which necessitates reciprocal respect among them. A parallel concept is also documented in the existing literature (Carrapico & Farrand,2024; Schmitt, 2017).

GGE reports have underscored that the most significant consequences can arise when a nation's critical infrastructure including hospitals, national security installations, energy systems, healthcare networks, and analogous entities subjected to cyber-attacks.

The agenda describes that member nations possess authority over ICT infrastructures located within their boundaries. The country exercises sovereign control over its own cyberspace. The same report emphasized that each State is sovereign over its territory while adhering to international law and respecting the sovereignty of other States. This implies an obligation to honor the rights of other nations. Furthermore, the report underscores the obligation of the State to refrain from intervening in the internal affairs of other member States; disputes between countries should be resolved through peaceful means. This principle highlights the preventative importance of the norm concerning the application of force and the preservation of international peace and security. Additionally, elements outlined in the agenda indicate that States are required to uphold and safeguard human rights and

fundamental freedoms; in this context, the enhancement of human rights, particularly freedom of expression, is deemed essential by the UN. The foundational principles of necessity, equilibrium, and differentiation are three vital cornerstones in the realm of global humanitarian law. The State is obligated to avoid utilizing information and communication technologies to facilitate actions that contravene international law and must ensure that non-state actors do not misuse its territory to execute such illicit activities. The EU Agenda based on the UN report advocates for the establishment of eleven voluntary and non-binding principles concerning responsible State conduct in relation to information and communication technologies (ICT). These principles encompass both affirmative and prohibitive obligations that are intended to curtail specific actions. The voluntary principles address a diverse array of matters, such as inter-State collaboration, attribution of ICT incidents, international misconduct, adherence to human rights, protection of critical infrastructure, supply chain integrity, the reporting of ICT vulnerabilities, and the functionality of emergency response teams.

Rule A: This principle underscores the significance of collaboration in the enforcement of all behavioral norms pertaining to responsible States. It aligns with the United Nations Charter, which articulates that the objectives of the United Nations include the adoption of "*effective collective measures for the prevention and removal of threats to peace" and "to achieve international cooperation in solving international problems. . .* ".

Standard B: This standard is designed to mitigate the likelihood of escalation in the event of a cyber incident. States are urged to act prudently following a cyber occurrence and to collect comprehensive information about the incident and its context prior to taking any measures. This standard further emphasizes the necessity of exercising discretion when attributing responsibility for an ICT incident. The realization of this standard is likely to necessitate the existence or establishment of mechanisms and procedures that facilitate cooperation among diverse institutions and stakeholders.

Norm C: This principle is derived from the UN report, which asserts that "S*tates must respect their international obligations regarding internationally wrongful acts attributable to them. Furthermore, States must not employ proxies to engage in internationally wrongful acts, and States should endeavor to ensure that their territories are not exploited by non-State actors for the unlawful application of ICTs*.

This rule relates to cyber incidents originating from a state's territory but not executed by that State itself. It may be impractical for a State to prevent all illicit usage of ICT infrastructure within its borders, especially given the disparate capabilities among States. However, if a State is cognizant of an internationally unlawful act utilizing ICT that originates from or is routed through its territory, and possesses the capacity to halt the malign activity, it should strive to do so in compliance with international law. In applying this rule, States could formally inform one another via National Points of Contact (PoCs) upon identifying such unlawful activities. This would not negate the accountability of the notified State for the activity, as it is feasible that the incident originated from a third State. States may contemplate employing standardized templates for notification purposes.
A State that becomes aware of harmful ICT activity originating from its territory but lacks the capability to respond may opt to seek assistance from other States.

Standard D: "States should intensify cooperation against the criminal or terrorist use of ICT, harmonize appropriate legal approaches, and strengthen practical collaboration between their respective law enforcement and judicial authorities. " [para. 22]

Norm E: "Initiatives undertaken by the state to mitigate ICT security challenges should be aligned with the upholding of human rights and essential freedoms as described in the Universal Declaration of Human Rights and other international agreements. " [see the UN Declaration of Human Rights,1948, para. 21]

Standard G: This standard pertains to the initiative-taking safeguarding of critical infrastructure. The second standard regarding critical infrastructure urges States to consider General Assembly Resolution 58/199 from 2003, which advocates for the establishment of a global culture of cybersecurity. This resolution delineates a collection of components essential for the protection of critical information infrastructure, which include:

• The establishment of emergency alert systems regarding cyber vulnerabilities, threats, and incidents.
• The enhancement of awareness among stakeholders to comprehend their responsibilities in safeguarding critical infrastructure.
• Identification of interdependence among critical infrastructures.
• Encouragement of collaborative efforts between public and private sectors to share and analyze information about critical infrastructure.
• Development and maintenance of crisis communication networks and regular testing.
• Execution of training and exercises to bolster response abilities.
• Implementation of legislation and training for personnel to investigate and prosecute attacks aimed at critical information infrastructure; and
• Participation in international cooperation, as deemed appropriate, for the protection of critical information infrastructures.

Standard H: Expanding upon prior standards, this standard introduces supplementary elements for a holistic strategy toward the protection of critical infrastructure. It stipulates that States should offer mutual support, upon request, in circumstances involving malicious ICT activities that impact critical infrastructure. Critical infrastructure encompasses essential functions that cross national borders and often necessitate international collaboration and support. The regulation also addresses the mitigation of detrimental ICT activities directed at another state's critical infrastructure, which originate from its own territory. In responding to such requests for assistance, States must take sovereignty considerations into account. Mechanisms for formulating and addressing these requests may be required, alongside precise information regarding the nature of the assistance required and the timing for its provision.

Standard I: This standard is based on the 2013 report that indicates, "States should encourage the private sector and civil society to participate appropriately in enhancing the security and utilization of ICT, including supply chain security for ICT products and services. " [para. 24]

This regulation encompasses three components:
• guarantee the integrity of the supply chain,

• avert the spread of detrimental ICT tools,
• obstruct the utilization of harmful hidden functions.

The primary objective of this standard is to foster trust and contribute to a global security culture in the deployment of ICT. It is essential to recognize that ICT tools generally possess dual-use capabilities: serving both legitimate and harmful intentions, and they are frequently readily accessible. Furthermore, there exists a potential for deliberate manipulation during the stages of development, implementation, or operation. There is also a possible risk of substitution with counterfeit components (including cloned or excessively produced items) before or during the delivery process. Thus, this standard aims to counteract the emergence of malicious hidden functionalities of ICT tools throughout the supply chain. It seeks to ensure the operational effectiveness of systems and services while fostering end-user confidence in ICT products and services.

Standard J: An ICT vulnerability fundamentally represents a flaw in a computer product or system that could enable an assailant to undermine its integrity, availability, or confidentiality. In simpler terms, it signifies a deficiency that permits an attacker to execute unauthorized actions within the computer product or system. This standard seeks to reduce the risk of malicious exploitation of ICT vulnerabilities. The exploitation of such vulnerabilities can result in substantial social, economic, political, and legal repercussions for societies. Consequently, this may lead to a degradation of user confidence in cyberspace overall, thereby compromising its principles of openness and interoperability, ultimately restricting its potential.

Threat actors can acquire so-called zero-day vulnerabilities without revealing them to the vendor or other pertinent organizations and can exploit them for malicious intentions at a later stage. Therefore, vulnerability information must be disclosed responsibly to avert its potential use for harmful purposes. Mitigating such vulnerabilities is a shared obligation of both the public and private sectors. This likely necessitates the creation of national frameworks or systems that facilitate responsible reporting and management of vulnerabilities, along with the exchange of information regarding possible remedies, and responsive coordination between public and private entities.

Norm K: The Computer Emergency Response Teams (CERTs) and Cyber Security Incident Response Teams (CSIRTs) serve as the primary responders tasked with alleviating the impacts of information and communication technology (ICT) vulnerabilities and harmful ICT behaviors affecting public, corporate, and governmental sector(see CERTs,2025; CSIRT,2025). Additionally, CERTs and CSIRTs might be empowered to support other governmental or non-governmental organizations in averting or lessening the impact of a forthcoming incident.

As the EU Cyber Security Agenda(2025) suggests, creating a National CERT may serve as a liaison both domestically and with other certifying bodies regionally and internationally. In this context, it is advisable for States to collaborate in enhancing and fortifying incident response capabilities and to promote cooperation between different CERTs. Furthermore, States should provide mutual assistance in reinforcing cooperative frameworks with national computer emergency response teams and other sanctioned emergency response organizations.

The objective of each of these structures is to safeguard and enhance the operational capability of CERTs and CSIRT to act as first responders consistently.

The operations of a national CERT can be categorized into two primary areas: reactive and proactive services (Ahmad & Hashim,2011). The principal reactive responsibilities of a national CERT include cyber incident management and analysis, incident response, and support. The proactive responsibilities pertain to the prevention of cyber incidents and include the development and upkeep of security tools, intrusion detection services, and the distribution of information and announcements regarding ICT vulnerabilities and incidents.

To execute its functions effectively, a national CERT should possess the following attributes:
- *Willingness to cultivate trust relationships*: The sharing of sensitive information is a critical element of a CERT's operations. A robust trust foundation can significantly enhance collaboration in both international and domestic scenarios.

- *Coordination*: The exchange of information and the response to incidents needs the involvement of numerous stakeholders at the national level. These stakeholders comprise the executive and legislative branches of government, the judiciary and law enforcement agencies, the intelligence community, operators and owners of critical infrastructure, vendors, and academic institutions. The CERT frequently acts as the intermediary among these parties regarding ICT issues. Many national CERTs develop competencies, such as incident response, containment, and service restoration. Nevertheless, these teams may often seek assistance from technical vendors or other CERTs for various aspects, rather than managing all functions independently. CERTs must adopt a proactive stance and extend their role beyond mere emergency response. They can provide a range of essential services aimed at comprehensive cybersecurity risk mitigation, including security training, development of security tools, and planning for disaster prevention and recovery (Meyer & Metille,2022; Ahmad& Hashim,2011).

- *Exchange of information regarding potential ICT threats*: By utilizing shared resources, organizations and entities can enhance their security by proactively leveraging the expertise, experience, and capabilities of their collaborators. The concept of enabling "*one organization's detection to become another's prevention*" represents a significant paradigm that can improve security for all.
- *Training, technology transfer, sustainability*: States ought to evaluate the most effective means of providing technical support to enhance ICT security capabilities and their application in nations seeking aid, particularly those in the developing world as the Western Balkans and Albania. Such initiatives may include:

• support and education aimed at enhancing security in the utilization of ICT, including critical infrastructure.
• sharing exemplary legal and administrative practices.
• aid in obtaining access to technologies considered vital for ICT security.
• dissemination of knowledge and technologies for the management of ICT security incidents.

Understanding and implementing the TALLINN MANUAL 2.0 on International cyber-operations

The 2007 assault on Estonia's essential infrastructure represented an unparalleled challenge to the collective defense principles of NATO member nations (NATO,2007). As a recent addition to the alliance, Estonia was highly interconnected, with its populace extensively engaging in online activities, including voting and banking. The denial-of-service attack that Estonia endured was among the most severe. At that time, the Estonian government attributed the attack to Russia, and Foreign Minister Urmas Paet sought NATO's support, expressing concerns that the extensive cyber-attack could jeopardize both the security of Estonia and that of the entire alliance. He invoked Article 5 of the Alliance Treaty, which outlines NATO's commitment to intervene to safeguard a member from the threat of an impending cyber conflict (Ashraf, 2021; Phongchiewboon, 2018). NATO member states at the time expressed concerns regarding the utilization of cyber tools; however, they did not perceive Article 5 as relevant to this situation. There had been no casualties or tangible damage to assets, thus providing insufficient grounds for initiating military action against Russia. The situation in Estonia underscored a disparity between antiquated legislation and the advent of emerging technologies, which failed to sufficiently safeguard a nation against cyber incursions. Consequently, NATO nations encountered challenges in assessing whether the assault on Estonia's infrastructure represented a cyber act of war. Presently, the matter of the legal framework governing cyberspace presents the issue that numerous contemporary laws are remnants of post-war agreements, such as the 1945 United Nations Charter and the 1949 Geneva Conventions, which are inadequate for the cyber realm. For instance, the definition of aggression does not encompass the cyberspace arena and pertains to the application of force against a state's territorial integrity (UN Charter, 1945). This definition poses challenges within the cyber context as it predicts that aggression transpires solely in the physical domain with delineated borders. However, cyber-attacks do not necessarily employ physical force, are not confined to specific geographic areas, and frequently involve non-state entities (Pongchiewboon, 2018, pp. 123). In 2009, the Tallinn Manual on International Law Applicable to Cyber Warfare was developed by a consortium of legal scholars appointed by the NATO Cooperative Cyber Defense Centre of Excellence (see CCDCE,2021). The purpose of the manual was to rectify regulatory deficiencies within cyberspace and to reconcile traditional international standards with contemporary technological advancements. The manual was developed as a non-binding document, categorized into essential rules and supportive comments. In the development of the manual, three organizations participated as observers: NATO, the International Committee of the Red Cross, and the United States Cyber Command. It is significant to highlight here that each rule and comment was reached by consensus among all authors, reflecting the diverse perspectives that emerged throughout the drafting and examination of the manual (Schmitt, 2013).

In February 2017, version 2. 0 of the Tallinn Manual was released, which enlarged and enhanced the exploration of the preceding version. The primary distinction between the two iterations pertains to the subject matter analyzed. The earlier manual predominantly addressed severe and destructive cyber operations, regarded as armed attacks that warranted a self-defense reaction by States, whereas the Tallinn Manual 2. 0 encompasses a broader spectrum of more general cyber operations that may transpire (Clark, 2024; Schmitt, 2013). Over the past decade, states have encountered persistent challenges arising from deleterious cyber activities, albeit these actions have not escalated to the threshold of warfare (Clark, 2024; Marsili, 2018). The examination of the Tallinn Manual encompasses its most recent iteration, referred to as the Tallinn Manual 2. 0, which is divided into

four distinct sections. The initial section relates to international law as it applies to cyberspace, the subsequent section addresses specialized regimes, the third section discusses international peace and security concerning cyber activities, and the final section reiterates the stipulations of the original Tallinn Manual regarding cyber-armed conflict. The Manual addresses various topics, including sovereignty, due diligence, jurisdiction, international liability, and cyber operations that remain unregulated by international law. Moreover, it delves into international human rights law alongside other specialized normative frameworks. The Manual also analyzes the peaceful resolution of disputes, the prohibition of intervention, and the criteria for the use of force (Clark, 2024; Marsili, 2018; Schmitt, 2013). A significant aspect addressed by the Manual is the principle of sovereignty, which is equally applicable to the domain of cyberspace. The differentiation between internal and external sovereignty is underscored, asserting that a State must refrain from engaging in cyber operations that infringe upon the sovereignty of another State (Marsili, 2018; Schmitt, 2013). Scholars contend that breaches of sovereignty within the cyber domain could constitute internationally unlawful actions, even though States have yet to unequivocally articulate their stances on this issue. The principle of due diligence requires States to implement measures that mitigate transboundary harm; however, the particulars of this principle and its implementation remain subjects of ongoing debate. The topic of due diligence has also been examined within the framework of the UN Group of Governmental Experts (GGE), albeit with limited engagement from States due to the associated responsibilities and practical challenges (Marsili, 2018). The Manual delineates that States may assert territorial and extraterritorial jurisdiction over cyber activities, bounded by the provisions of international law. Jurisdiction may be exercised within national borders in both prescriptive and enforcement scenarios, whereas the scope abroad is comparatively limited. International collaboration is crucial, as jurisdictions may overlap (Schmitt, 2013). The Tallinn Manual, despite commonly being misidentified as a NATO Manual, is a product of independent academic inquiry. While its origins stem from the exigencies and experiences of NATO, the Manual is characterized by its distinct nature. It does not reflect the views of the participating nations, but rather those of specialists in international law within the cybersecurity context. It is regarded as one of the pioneering and most significant attempts to comprehend and elucidate international law in the cyber domain, thereby shaping the perspectives and approaches of States regarding these matters in the future. Although classified as academic research rather than an international law treatise, it has faced criticism concerning its practical applicability. Some detractors question whether the Tallinn Manual serves merely as a "book of rules on the shelf. " Several criticisms have emerged against the proposed regulations and interpretations of the Manual. Firstly, it remains uncertain whether States have endorsed or are prepared to embrace the Tallinn rules, based on their actions within the cyber sphere or on formal national policies. Secondly, states frequently maintain silence regarding their operations in cyberspace, revealing a tenuous interest in fostering legal certainty in this domain. This is attributed to the apprehension of states regarding increased vulnerability and diminished transparency in the perception of others.

Scholars concur that the customary law regarding state liability applies to cyber activities. Physical harm does not need to occur for cyber action to be deemed internationally wrongful. Attributing responsibility to non-state actors remains a complicated matter. Cyber operations employed as countermeasures raise concerns regarding temporal considerations and proportionality. A category of unregulated cyber activities exists, including cyber espionage in times of peace. The implications of international human rights law have been extensively debated, as its relevance to cyber activities

necessitates independent evaluation. The obligation of States to safeguard human rights is a contentious issue within the international community. Additionally, States must weigh other obligations such as national security, which may restrict the application of international human rights law. The section about international peace and security discusses the principle of resolving disputes peacefully and the prohibition of intervention. Perspectives on the effective range of the prohibition of intervention are varied. Experts assert that the United Nations should refrain from intervening through cyber means in the internal affairs of States (Clark, 2024). Exceptions are permitted for the implementation of measures mandated by the UN Security Council under Chapter VII of the United Nations (see CCDCE,2021). The original Tallinn Manual offers insights regarding the use of force. The principal challenge lies in ascertaining whether cyber-attacks indeed qualify as a use of force, due to the intricate nature of interpreting occurrences in the digital realm. Specialists have formulated a set of criteria to juxtapose cyber-attacks with the repercussions of armed conflict. The criteria encompass the gravity of the effects, their immediacy, the velocity of the attack, the invasive nature, the measurability of the impacts, the involvement of the State in cyber activities, and the presumed compliance with international law (Tanodomdej, 2019). States operate covertly within the cyber realm, generating uncertainty and selectively applying international legal standards. There is a reluctance to embrace the provisions outlined in the Tallinn Manual, as states fear these may not sufficiently safeguard their long-term interests. Nonetheless, there is an imperative to establish regulatory frameworks for international law in cyberspace; however, lawmakers exhibit reluctance in addressing this issue due to its far-reaching ramifications. Disparities and ambiguities regarding legal principles in the cyber domain persist among experts and states. The Tallinn Manual 2. 0 is expected to serve as a foundational reference for forthcoming advancements in cyber law. Certain states may perceive a degree of threat stemming from the absence of international regulations and constraints on the utilization of information and communication technologies (ICT) by other states or non-state entities. The enhancement of confidence and trust among states is essential and can be achieved through the eleven voluntary norms of behavior established by the GGE-UN and specific confidence-building measures (CBM) such as ***inter-state communication and improved dialogue***, particularly aimed at mitigating risks of misinterpretation, escalation, and conflict. Such initiatives can be implemented at bilateral, regional, sub-regional, and multilateral levels. The UN-GGE also advocates for workshops, seminars, and exercises to refine national considerations on incident prevention.

A consistent institutional dialogue to reinforce shared understandings and elevate practical collaboration with extensive participation, particularly under the United Nations framework. This communication should incorporate ongoing processes and designated interlocutors in both technical and political spheres. ***Equally significant*** as identifying points of contact and determining information-sharing protocols is the capacity to convey information unambiguously, thereby minimizing potential misconceptions. By the recommendations from Government Expert Group reports, the facilitation of information exchange may be enhanced through voluntary national agreements that classify ICT incidents according to their scale and severity. For instance, the National Cyber Security Centre in the UK employs a cyber-attack categorization system aimed at bolstering national incident response capabilities. This system encompasses six incident categories, emphasizing their national implications. At the lowest echelon, Category 6, incidents are confined to a local context. Conversely, at the highest level are incidents that produce prolonged disruptions to vital national services or threaten national security, resulting in considerable economic or social ramifications, or even loss of life. Such classifications may also apply to international incidents,

proving beneficial for the transmission of critical information to other national entities or governments, such as the degree of severity of a particular incident, the immediacy required for response action, the expertise necessary to coordinate response initiatives, and the financial investment demanded by these efforts. Member States have the authority to formulate their own classification systems and subsequently seek to harmonize them through dialogue with other nations at both regional and global levels.

A further category of confidence-building measures pertains to transparency. Transparency fosters trust through, for example, the provision by states of national perspectives and information regarding emerging threats, infrastructure deemed critical, and national initiatives to safeguard such infrastructure, alongside the interchange of information on national strategies. The annual report of the Secretary-General of the United Nations addressing developments within the information and telecommunications sector in the realm of international security has already tackled this matter via a compilation of national viewpoints submitted by States. In the report, United Nations Member States are encouraged to convey to the Secretary-General their perspectives and evaluations regarding the following inquiries:

• Overall evaluation of information security challenges.
• initiatives implemented at the national level to enhance information security and foster international collaboration in this domain.
• The substance of international frameworks designed to bolster the security of global information and telecommunication infrastructures.
• Potential actions [that could be undertaken] by the international community to enhance information security on a global scale.

Recent Secretary-General reports can be accessed on the website of the United Nations Office for Disarmament Affairs (UNODA, 2023).
The UN-GGE advocates for States to disclose their perceptions of categories of essential infrastructure as well as the measures they are employing to safeguard them.
Examples of critical infrastructure comprise:
the chemical industry
the commercial infrastructure sector
• the communications domain
• the essential manufacturing sector
• the dam infrastructure
• the primary defense industrial sector
• the emergency services domain
• the energy industry
• the financial services sector
• the agri-food industry
• the governmental facilities sector
• the health and public health sector
• the information technology field
• the nuclear reactors, materials, and waste sector
• the transport infrastructure sector

• the water and sewage sector.

An additional approach to foster collaboration and confidence, both domestically and with external partner nations, is through the facilitation of cybersecurity drills as a preventive and planning strategy ensuring that appropriate mechanisms and frameworks are established in the event of a cybersecurity incident.

These dialogues engage states, while others encompass wider participation from civil society, industry, and academic spheres. Although some may not specifically target the enhancement of trust among states, they primarily aim at fostering dialogue and consensus on normative and practical matters. Such initiatives can cultivate trust between states in ways that should not be overlooked.The GGE reports underscore that countries hold the primary responsibility for safeguarding national security as well as the well-being of their citizens within the Information and Communications Technology (ICT) domain. Nonetheless, numerous nations possess inadequate capabilities to secure their ICT infrastructure. This deficiency can render both citizens and critical infrastructure vulnerable to risks associated with ICT activities. The final significant focus addressed by the GGE reports pertains to international collaboration and support concerning ICT security and capacity building (CAPB). Broadly, nations ought to "*strive to create a global culture of cybersecurity*" (see General Assembly Resolution 64/211).

The expansive field of international collaboration aimed at enhancing global security capabilities is referred to as Cyber Capability Building (CCB). A more contemporary definition describes CCB as "a means to empower individuals, communities, and governments to fulfill their development objectives by mitigating digital security threats linked to the use and access of information and communication technologies" (Creese et al., 2021).

The principles constituting the CCB encompass fundamental and intricate elements:
1. *Raising awareness and educating* individuals regarding the significance of cybersecurity. This entails promoting responsible digital conduct, enhancing awareness of prevalent cyber threats, and offering training programs aimed at augmenting cybersecurity competencies.
2. *Policy and Governance* and the establishment of robust policies and governance is vital for effective cyber capacity development. This encompasses the delineation of roles and responsibilities, the formulation of cybersecurity strategies and plans, and the implementation of regulations and standards to direct cybersecurity practices.
3. *Technical Infrastructure*: The development of cyber capabilities necessitates the construction of a resilient technical infrastructure. This involves the deployment and maintenance of secure network architectures, the implementation of firewalls, intrusion detection systems, and other security mechanisms, along with ensuring that hardware and software remain current.
4. *Incident Response and Management*: Cultivating the capability to respond to and proficiently manage cyber incidents is a crucial component of enhancing cyber capacity. This includes the establishment of incident response plans, the formation of incident response teams, and the conduction of regular drills and exercises to assess and enhance response proficiency.
5. *Collaboration and Partnerships*: The augmentation of cyber capacity frequently necessitates collaboration and partnerships with a variety of stakeholders. This may encompass cooperation

among government entities, private sector organizations, academic institutions, and international partners to exchange information, expertise, and best practices.
6. *Research and Development*: Allocating resources to research and development is vital to staying abreast of the evolving landscape of cyber threats. This comprises investigating emerging technologies, vulnerabilities, and attack methodologies, as well as developing innovative solutions to confront these challenges.
7. *Continuous Improvement* (lessons learned): The enhancement of cyber capabilities is an iterative process demanding ongoing refinement. This involves monitoring and assessing the efficacy of cybersecurity measures, deriving lessons from prior incidents, and modifying strategies and practices to address new threats.

The Cybersecurity Strategy of the European Union (2025) outlines objectives aimed at aiding the EU's partners in enhancing their cybersecurity capabilities. This external initiative must be understood within the global discourse regarding cyber norms. In November 2021, the EU adopted the Paris Call for Trust and Security in Cyberspace, supplementing the prior endorsements from all 27 of its Member States (see the Paris Call for Trust and Security in Cyberspace, 2018). The signatories of the Paris Call advocate for “open, secure, stable, accessible and peaceful cyberspace" and express their commitment to implementing collaborative measures by the nine principles outlined in the Paris Call. Consequently, it is expected that the 2020 Strategy will endorse these principles, although the Paris Call underscores the importance of security through a flexible methodology.

Given that international collaboration and support are critical for achieving global ICT security and resilience, the international community must unite to offer mutual assistance, particularly to developing yet rapidly growing nations:

- to enhance the security of essential ICT infrastructures.
- to cultivate technical expertise and establish relevant legislation, strategies, and regulatory frameworks to fulfill their responsibilities.
- to address disparities among States in terms of ICT security and utilization.

Criminal Law Regulation in some European Nations

The significant societal threat posed by cybercrimes and the persistent rise in the exploitation of computer systems necessitates the establishment of specific legal frameworks to address this issue. Consequently, there is a demand for new amendments to the criminal codes that will impose penalties for such criminal activities. To mitigate computer-related offenses, numerous nations are endeavoring to identify the most effective strategies, methodologies, and measures. Primarily, the regulation of criminal law should be viewed as a safeguard against unauthorized access to computer systems. Following the enactment of laws about the criminalization of illegal access to computer systems, extensive discussions among lawmakers have occurred regarding the point at which this unauthorized access should be classified as a criminal act. Therefore, various nations consider it a criminal offense from the initial unauthorized access, while others recognize it as such only when a minimal level of damage is inflicted (Payne, 2020). Traditional criminal law provisions have failed to adequately ensure protection against unauthorized access to computer systems; hence, the European Union and a number of its member states have instituted new legislation aimed at establishing punitive measures for cybercrimes that impact society. The provisions within the criminal laws of Great Britain illustrate

that various forms of cybercrime have been integrated following recommendations from the Council of Europe. In 1990 and the latest amendments of 2020, the United Kingdom enacted the Computer Misuse Act, which delineates particular cyber offenses (see Criminal Law Act of Great Britain,2020). This legislation addresses criminal activities encompassing a broad spectrum of computer misuse, including deliberate actions undertaken by the offender, such as computer fraud and computer sabotage, with the intent to exploit data, software, or the computer system itself (Payne, 2020). The Austrian criminal law lacked explicit provisions concerning the penalization of cybercrime until the year 1987. In connection with the legal transformations and latest amendments of 2024, the insights provided by the idea that "*in the course of reforming the Austrian Criminal Code, criminal liability ought to be expanded to include further offenses, such as hacking, by a forward-looking societal framework* "were endorsed. For violations within this field, sanctions of up to 2 years of incarceration or monetary fines are prescribed, while the identical offense, when executed under specific qualifying circumstances, may attract a prison term ranging from 6 months to 5 years (Austrian Criminal Code as amended, 2024). The evolution of the legal and criminal frameworks relating to cybercrime has progressed similarly in Germany, reflecting trends observed in various developed nations, particularly through the introduction of amendments to the existing Criminal Code that establish new sections addressing criminal activities within the domain of computer crimes. In 1986, legislation aimed at the prevention of economic crime was enacted, which integrated offenses about computer crime such as data theft, computer fraud, falsification of data critical to evidentiary processes, and computer sabotage. Criminal sanctions for these specified offenses range from 1 to 5 years of imprisonment, alongside the imposition of fines in the latest amendments of 2021(Criminal Code of the Federal Republic of Germany, revised, 2021). In Canada, Section 342/1 of the Criminal Code categorizes cybercrime as an offense punishable by a maximum sentence of 10 years (Consolidated Federal Laws, Criminal Code of Canada, 2024). The French Criminal Code, effective since 1993, delineates cybercrime offenses in Sections 182, 323/1, and 323/4, encompassing unauthorized data collection, computer fraud, fabrication of computer data, and the obstruction of computer system operations, which attract penalties of fines and imprisonment lasting from 1 to 3 years (French Code of Criminal Procedure Act, 2020). The Polish Criminal Code aligns its treatment of cybercrime offenses with the recommendations set forth by the Council of Europe, prescribing a term of imprisonment exceeding 8 years for unauthorized access to a computer system, computer data interception, and sabotage. The dissemination of information obtained through illegal means is penalized with 2 years of imprisonment (Polish Criminal Code, 1997).

Criminal provisions of the cybercrime offenses in Albania: A legal examination

Albania ranks among the countries where the development of telecommunications, internet access, and the digitalization of society is progressing very rapidly.

The adoption of a series of laws in this field, such as Law No. 9880 of 25.02.2008 "*On Electronic Certification*," Law No. 9918 of 19.05.2008 "*On Electronic Communications in the Republic of Albania*," Law No. 10128 of 11.05.2009 "*On Electronic Commerce*," Law No. 10325 of 23.09.2010 "*On State Databases*," Law No. 103/2024 of 19.09.2024 "*On the Organization and Functioning of the National Geospatial Information Infrastructure in the Republic of Albania,*" and a series of subordinate acts following them, have legally sanctioned Albania's inclusion in this new global approach(see Law No.9880; Law No.9910; Law No. 10128; Law No.10325; Law No.103/2024 of the Republic of Albania). In 2002, Albania signed the Council of Europe Convention through Law No. 8888 of the 25.04.2002 "*On the Ratification of the Convention on Cybercrime*."

The Cybercrime Investigation Department within the General Prosecutor's Office was created with approximately 10 prosecutors from the Serious Crimes Prosecutor's Office, and the Cybercrime Sector was established in the General Directorate of Police under the Economic Crime Department to examine 18 criminal offenses delineated in the Criminal Code.
In 2011, the Albanian Government established the National Agency for Computer Security through Decision No. 766 of 24.09.2011.

The Albanian government has additionally prepared a set of policy and strategic laws, particularly the creation of a national strategy for cybersecurity and the prioritization of cybersecurity as a significant risk within the National Security Strategy (Law No. 14/2024 of the 31.07.2014 "*On the Approval of the National Security Strategy of the Republic of Albania*"). Simultaneously, this approach was further reinforced with the Cybersecurity Policy Protocol approved through Decision No. 973 of 02.12.2015, considering that since Albania's membership in NATO, critical cyber infrastructures for the circulation and exchange of information between various security agencies or external services have become essential.

The country has adopted Law No. 107 of the 15.10.2015 "*On Electronic Identification and Trusted Services*," as amended; Law No. 2/2017 "*On Cybersecurity*" and Law No. 10/2023 "*On Classified Information*."

In the context of Albania's integration into the European Union, the country provides updates on cybersecurity components under Chapter *X "Information Society*," while addressing cybercrime in Chapter XXIV, which relates to issues of national security. Albania has made significant advancements in the Global Cybersecurity Index for the year 2024, progressing from an evolving nation to an advancing Tier 2 classification. The nation has attained a score of 20 out of 20 in legal measures, 18. 38 out of 20 in technical measures, 19. 47 out of 20 in organizational measures, 12. 08 out of 20 in capacity building, and 16. 58 out of 20 in cooperation measures. Areas such as capacity enhancement and collaboration demonstrate opportunities for additional improvements. The General Prosecutor's Report on the status of criminal activity in Albania for 2023 indicates that cybercrime accounts for 1. 9% of the overall criminal proceedings documented and has experienced a rise of 22. 35% compared to 2022 (Report of the General Prosecutor's Office on Criminality, 2023, pp. 146). Although this percentage is minor relative to other criminal activities, there is a noticeable increasing trend in instances of cybercrime over the years.

In the Albanian Criminal Code, several articles provide for cyber-related criminal offenses, which are not consolidated in a specific section but can be found throughout the code:

- **Article 74/a** - *Computer Distribution of Genocide or Crimes Against Humanity Materials.* This article addresses the dissemination of materials via computer that promote or rationalize actions constituting genocide or crimes against humanity. It renders two forms of conduct criminal: *public offering and intentional distribution to the public through digital platforms*. The materials being disseminated must significantly deny, trivialize, endorse, or rationalize actions that are classified as genocide or crimes against humanity. This article underscores

Albania's robust position against the advocacy or justification of such acts and acknowledges the necessity of regulating online conduct.

- **Article 84/a** - *Harassment Motivated by Racism and Xenophobia Through Computer Systems.* This article, incorporated by Law No. 10 023 of 2008, regards the racial and xenophobic threats disseminated via informatic systems. It penalizes grave threats to take the life of or harm an individual due to their ethnicity, nationality, race, or religion, with penalties including a fine or a prison sentence of up to three years. This regulation recognizes the detrimental impacts of such threats and demonstrates the Albanian government's dedication to combating these issues.

- **Article 119/a**/b - *Distribution of Racist or Xenophobic Materials Through Computer Systems.* This article focuses on the distribution of racist or xenophobic materials through informatic systems, criminalizing the offering or intentional distribution of such content. It recognizes the role of technology in spreading hate speech and discriminatory messages.

- **Article 143/b** - *Computer Fraud*. This article sanctions the criminal offense of computer fraud, involving actions aimed at economic gain through deception or harm to others. These actions include inputting, altering, deleting, or removing computer data or interfering with the operation of an informatic system

- **Article 186/a** - *Computer Forgery*. This article provides for the criminal offense of manipulating computer data, specifically the unauthorized input, alteration, or deletion of computer data. It becomes more severe when manipulated data is used as authentic data.

- **Article 192/b** - *Unauthorized Access*. This article sanctions the criminal offense of unauthorized access to a computer system or part of it, in violation of its security measures. It aims to protect critical computer systems from unauthorized access, which could cause serious harm to national security, public order, or public health.

- **Article 293/a** - *Unlawful Interception of Computer Data*. This article, added by Law No. 10 023 of 27.11.2008, criminalizes the unlawful interception of non-public transmissions or computer data from or within a computer system, punishable by three to seven years of imprisonment. If committed within the military, national security, public order, or civil defense systems, the penalty increases to seven to fifteen years.

- **Article 293/b** - *Interference with Informatic Data*. This article, added by Law No. 10 023 of 27.11.2008, criminalizes unauthorized damage, distortion, alteration, deletion, or suppression of computer data, punishable by six months to three years of imprisonment. If committed on military, national security, public order, or civil defense data, the penalty increases to three to ten years.

- **Article 293/c** - *Interference with Computer Systems*. This article, added by Law No. 10 023 of 27.11.2008, criminalizes the creation of serious and unauthorized obstacles to impair the functioning of a computer system, punishable by three to seven years of imprisonment. If

committed to the military, national security, public order, or civil defense systems, the penalty increases to five to fifteen years.

- **Article 293/ç** - *Misuse of Devices*. This article, added by Law No. 10 023 of 27.11.2008, criminalizes production, possession, sale, distribution, or any other action making available a device, including computer software, password, access code, or similar data, created or adapted for unauthorized access to a computer system, punishable by six months to five years of imprisonment.

- **Article 293/d** - *Unauthorized Sale of SIM Cards*. This article, added by Law No. 98 of 31.07.2014, criminalizes the violation of rules for the distribution, sale, and provision of SIM cards/products, punishable by thirty days to six months of imprisonment.

CONCLUSIONS

Global societies are increasingly drawn to the significant advantages offered by information and communication technology, prompting governments in developed nations to allocate resources towards this sector. It is crucial to safeguard these benefits, which are vital for national security, from potential cyber threats.

Overall, this research endorses a unified approach toward the structures proposed in developed nations and elucidates how these countries have effectively addressed cybersecurity concerns. Albania's national cyber defense strategy must incorporate the most effective methods and models, many of which have been successfully implemented in developed nations. Strategies and programs must be tailored to align with the specific needs and preparedness of the nation for their implementation, while also anticipating the future requirements of the country. An optimal approach for Albania as a country in the micro-analysis and the European Union in the macro-analysis would involve the development of cybersecurity capabilities and central units at the point in time when they are most essential and urgently needed.

- The strategic goals that should be pursued to realize this vision include:
1. Finalizing the legal framework for cybersecurity.
2. Enhancing awareness concerning cybersecurity.
3. Improving knowledge, skills, and capacities pertinent to expertise in the cybersecurity domain.
4. Establishing specialized units.
5. Identifying and safeguarding Critical Information Infrastructures (CIIP).
6. Designing and executing fundamental cybersecurity requirements.
7. Augmenting investments to bolster security within governmental networks/systems.

REFERENCES

Adeyeri, A., & Abroshan, H. (2024). Geopolitical ramifications of cybersecurity threats: State responses and international cooperations in the digital Warfare era. *Information*, *15*(11), 682. https://doi.org/10.3390/info15110682

Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2023). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, *2*, 100031. https://doi.org/10.1016/j.csa.2023.100031

Ahmad, R. A. & Hashim, M. S. Computer Emergency Response Team(OIC-CERT): Answering cross border cooperation. (2011) *Second Worldwide Cybersecurity Summit (WCS)*, London, UK, pp. 1-5

AlSalem, T., Almaiah, M., & Lutfi, A. (2023). Cybersecurity Risk Analysis in the IoT: A Systematic review. *Electronics*, *12*(18), 3958. https://doi.org/10.3390/electronics12183958

Ashraf, C. (2021). Defining cyberwar: towards a definitional framework. *Defense and Security Analysis*, *37*(3), 274–294. https://doi.org/10.1080/14751798.2021.1959141

Boeke, S. (2017). National cyber crisis management: Different European approaches. *Governance*, *31*(3), 449–464. https://doi.org/10.1111/gove.12309

Carrapico, H., & Farrand, B. (2024). Cybersecurity trends in the European Union: regulatory mercantilism and the digitalisation of geopolitics. *JCMS Journal of Common Market Studies*. https://doi.org/10.1111/jcms.13654

Clark, I. (2024). International Research cooperation in the Tallin Manual. *Granite*, 1–19. https://doi.org/10.57064/2164/24388

Creese, S., Dutton, W. H., Esteve-González, P., & Shillair, R. (2021). Cybersecurity capacity-building: cross-national benefits and international divides. *Journal of Cyber Policy*, *6*(2), 214–235. https://doi.org/10.1080/23738871.2021.1979617

Marsili, M. (2018). The war on cyberterrorism. *Democracy and Security*, *15*(2), 172–199. https://doi.org/10.1080/17419166.2018.1496826

Meyer, P., & Métille, S. (2022). Computer security incident response teams: are they legally regulated? The Swiss example. *International Cybersecurity Law Review*, *4*(1), 39–60. https://doi.org/10.1365/s43439-022-00070-x

Payne, B. K. (2020). Defining cybercrime. In *Springer eBooks* (pp. 3–25). https://doi.org/10.1007/978-3-319-78440-3_1

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing Cybercrime: Definitions, typologies and taxonomies. *Forensic Sciences*, *2*(2), 379–398. https://doi.org/10.3390/forensicsci2020028

Phongchiewboon, A. (2018). Book review: Cybersecurity and Cyberwar: What Everyone needs to know. *SSRN Electronic Journal*. https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3318132_code2732908.pdf?abstractid=3318132&mirid=1

Schmitt, M. N. (2013). Tallinn Manual on the international law applicable to cyber warfare. In *Cambridge University Press eBooks*. https://doi.org/10.1017/cbo9781139169288

Tanodomdej, P. (2019). The Tallinn Manuals and the making of the International Law on Cyber Operations. *Masaryk University Journal of Law and Technology*, *13*(1), 67–86. https://doi.org/10.5817/mujlt2019-1-4

Computer Emergency Response Team CERT-AGID. (2025). CERT-AGID. https://cert-agid.gov.it/

Computer Security Incident Team CSIRT. (2025). https://www.csirt.org/

European Union Agency on Cybersecurity (ENISA). (2025, January 17). https://www.enisa.europa.eu/publications

North Atlantic Treaty Organization (NATO). (2007). *Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective*. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfare Perspective.pdf

The cybersecurity strategy. (2025, January 15). Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

The International Telecommunication Union (ITU). (2024). *Global Cybersecurity Index 2024 5th Edition*. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

The NATO Cooperative Cyber Defence Centre of Excellence. (2021). *The Tallinn Manual 2.0*. https://ccdcoe.org/research/tallinn-manual/

Universal declaration of human rights. (1948, December 10). https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf

United Nations. (2002, December 20). *Resolution adopted by the General Assembly [on the report of the Second Committee (A/58/481/Add.2)]*. https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf

United Nations. (1945). *UN Charter | United Nations*. https://www.un.org/en/about-us/un-charter Article 2, Paragraph 4

UNODA – United Nations Office for Disarmament Affairs. (2023). https://disarmament.unoda.org/

Legal Acts

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Network and Information Security: Proposal for a European Policy Approach (COM(2001)298 final). (2001). https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0298:FIN:EN:PDF

Convention on Cybercrime of Budapest (No.185). (2001). https://rm.coe.int/1680081561

Criminal law of Austria. (2024, June 17). oesterreich.gv.at - Österreichs Digitales Amt. https://www.oesterreich.gv.at/en/themen/gesetze_und_recht/strafrecht.html

Criminal Code of Poland. (1997). https://sherloc.unodc.org/cld/uploads/res/uncac/LegalLibrary/Poland/Laws/Criminal%20Code%20(Poland).pdf

Criminal Law Act 1977 of the Great Britain. (2020). https://www.legislation.gov.uk/ukpga/1977/45/2020-12-31

CRIMINAL PROCEDURE CODE OF THE REPUBLIC OF ALBANIA. LAW No.7905, 21 Mar. 1995, Articles 74/a, Article 84/a, Article 119 a/b, Article 143/b, Article 186/a, Article 192/b, Article 293/a, Article 293/b, Article 293/, Article 293/ç, Article 293/d https://legislationline.org/sites/default/files/2023-09/criminal%20code%20of%20albania.pdf

DECISION ON THE APPROVEMENT OF THE CYBER SECURITY POLICY DOCUMENT 2015 - 2017[V E N D I m MIRATIMIN e DOKUMENTIT TË POLITIKAVE PËR SIGURINË KIBERNETIKE 2015 - 2017] (No. 973). (2015). https://aksk.gov.al/wp-content/uploads/2020/07/Dokumenti-i-Politikave-per-Sigurine-Kibernetike-2015-2017.pdf

Directive on Security of Network and Information Systems (NIS Directive) EU Cybersecurity Policy(2018).. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/654198/EPRS_BRI(2020)654198_EN.pdf

Document summary | Legislative Observatory | European Parliament Resolution No. 2013/2606. (2013). European Union- Source: European Parliament. https://oeil.secure.europarl.europa.eu/oeil/en/document-summary?id=1281396

German Criminal Code (Strafgesetzbuch – StGB). (2021). https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html

HIGH REPRESENTATIVE OF THE EUROPEAN UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY. (2013). *OINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (JOIN(2013) 1 final). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001

Law on the Organization and Functioning of the National Geospatial Information Infrastructure in the Republic of Albania [Ligj PËR ORGANIZIMIN DHE FUNKSIONIMIN e INFRASTRUKTURËS KOMBËTARE TË INFORMACIONIT GJEOHAPËSINOR NË REPUBLIKËN e SHQIPËRISË] (No. 103/2024). (2024). https://asig.gov.al/wp-content/uploads/2024/10/Ligji_nr_72_2012_Per_organizimin_dhe_funksionimin_e_Infrastruktures_Kombetare_te_Informacionit_Gjeohapesinor_ne_Republiken_e_Shqiperise_i_perditesuar.pdf

LAW ON THE APPROVAL OF THE NATIONAL SECURITY STRATEGY OF THE REPUBLIC OF ALBANIA [LIGJ PËR MIRATIMIN e STRATEGJISË SË SIGURISË KOMBËTARE TË REPUBLIKËS SË SHQIPËRISË] (No. 14/2024). (2024). https://qbz.gov.al/eli/ligj/2024/02/08/14/6f7aeb09-5b35-4f1b-83a8-bab03464a153;q=strategj

Law on Electronic Communications in the Republic of Albania [Ligj per komunikimet elektronike ne Republiken e Shqoiperise] (No.9918). (2018). https://www.infrastruktura.gov.al/wp-content/uploads/2021/11/Ligj_9918_19-05-2008-perditesuar-me-Ligjin-102_24-10-2012-me-Ligjin-107-dt.-20.12.2018.pdf

Law on Cybersecurity [LIGJ PËR SIGURINË KIBERNETIKE] (No. 2/2017). (2017). https://aksk.gov.al/wp-content/uploads/2023/07/ligj-2017-01-26-2.pdf

Law on Electronic Identification and Trusted Services [LIGJ PËR IDENTIFIKIMIN ELEKTRONIK DHE SHËRBIMET e BESUARA] (No.107). (2015). https://aksk.gov.al/wp-content/uploads/2023/07/ligj-2015-10-01-107.pdf

Law on State Databases [Ligj per bazat e te dhenave shteterore] (No.10325). (2010). https://qsha.gov.al/wp-content/uploads/2024/10/1-ligj-nr-10325-dt-23.09.2010-per-bazen-e-te-dhenave-shteterore.pdf

Law on Electronic Commerce [LIGJ PËR TREGTINË ELEKTRONIKE] (No.10128). (2009). https://aida.gov.al/wp-content/uploads/2023/12/Ligji_10128_per_Tregtine_Elektronike_i_ndryshuar.pdf

Law for electronic Certification in the Republic of Albania [Ligji per Nenshkrimin Elektronik ne Republiken e Shqiperise] (Law No.9880) (2008). https://qbz.gov.al/eli/ligj/2008/02/25/9880

Law for the ratification of the "Convention on Cybercrime" [Ligj per ratifikimin e konventes per krimin ne fushen e kibernetikes]ntes ne fushen (No.8888). (2002). https://qbz.gov.al/eli/ligj/2002/04/25/8888

Legislative Services Branch. (2024b, October 10). *Consolidated federal laws of Canada, Criminal Code*. https://laws-lois.justice.gc.ca/eng/acts/c-46/

Official Journal of the European Union. (2009). *DIRECTIVE 2009/140/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL* (L 337/37). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0140

Resolution adopted by the General Assembly on 21 December 2009 (A/RES/64/211). (2010). United Nations. https://docs.un.org/en/A/RES/64/211

Report of the General Prosecutor on criminality for the 2023 [Raport i prokurorit te pergjithshem per gjendjen e kriminalitetit per vitin 2023]. (2024). https://www.pp.gov.al/rc/doc/Raporti_1_PP_2023_date_28_03_2024_7383.pdf