FUTURITY
Economics & Law

DOI: https://doi.org/10.57125/FEL.2022.03.25.01

How to cite: Gushchyn, O., Kotliarenko, O., Panchenko, I., & Rezvorovych, K. (2022). Cyber Legislation in Ukraine: Current Status and Development Prospects. *Futurity Economics & Law, 2*(1), 4–19. https://doi.org/10.57125/FEL.2022.03.25.01

Cyber Legislation in Ukraine: Current Status and Development Prospects

Oleg Gushchyn*

PhD in Law, Professor, Military Law Department, Taras Shevchenko National University of Kyiv, Military Institute, Kyiv, Ukraine, https://orcid.org/0000-0003-2901-9605

Oleksandr Kotliarenko

PhD in Law, Deputy Head, Military Law Department, The National Defense University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine, https://orcid.org/0000-0001-8776-2515

Iryna Panchenko

Doctor of Law, Associate Professor, Department of Economics and Maritime Law, Kherson State Maritime Academy, Kherson, Ukraine, https://orcid.org/0000-0003-4545-3794

Krystyna Rezvorovych

Doctor of Juridical Sciences, Head, Department of Civil Law and Procedure, Faculty of Training Specialists for Criminal Police Units, Dnipropetrovsk State University of Internal Affairs, Dnipro, Ukraine, https://orcid.org/0000-0003-1183-613X

***Corresponding Author:** *o_guschyn@knu.ua.*

Received: October 26, 2021 | **Accepted:** January 8, 2022 | **Published:** March 25, 2022

Abstract: This work examines the cyber law framework of Ukraine by focusing on its effectiveness in mitigating cyber threats amid ongoing geopolitical challenges. The analysis is done by examining the data from the State Service of Special Communications and Information Protection of Ukraine, legal documents, and expert interviews. The research reveals that while significant progress has been made with new laws and amendments, enforcement remains a critical issue. From 2017 to 2021, cyberattacks

increased by 86% in the country. That are particularly targeting critical infrastructure. Despite robust legislative measures, only 33% of reported incidents result in successful prosecutions. Moreover, there a notable inefficacy in enforcement and coordination among regulatory bodies is found. Furthermore, the business sector surveys indicate moderate satisfaction with legal protections and regulatory responses. Also, the descriptive statistics indicate moderate satisfaction with legal protections (mean 3.2) and regulatory responses (mean 3.5) while business representatives report substantial financial impacts from cyber incidents. Correlation analysis shows a strong negative relationship between the number of cyberattacks and prosecution success rate (r = -0.85) suggesting that increased cyberattacks are associated with lower prosecution success. The study concludes with recommendations for enhancing coordination, improving enforcement, and aligning with international best practices. This will ensure betterment in the Ukraine's cybersecurity resilience and address the evolving cyber threat.

Keywords: Business sector, cyber law, cybersecurity, geopolitical challenges, international collaboration, legal framework, Ukraine.

Introduction

In the digital era, cybersecurity has turned into a critical element of national security and economic wellbeing (Reveron & Savage, 2020). As governments continue to depend on their largely online systems, not only do cyber laws need to be enforced more strictly Sule et al. (2021) but also the complex digital infrastructures require protection from such threats. Ukraine is facing real Geopolitical hurdles. Creating and enforcing comprehensive cyber laws would keep digital assets and infrastructure safe (Zahorulko, 2020). Ukraine has experienced rapid digitalization in recent years, with the expansion of online services, e-commerce and transition to electronic governance. The increased interest of governments and the private sector to enhance digital health also reflects a broader global tendency where cybersecurity is poised for primacy. The main purpose in protecting and security is to minimize the dangerous effects of cyber-attacks, as much as possible with Ukraine´s digital development systems (Zaichuk & Zaichuk, 2019). Ukraine has been a good actor in the context of cyber defense, actively taking part in international cooperation and applying global principles (Romaniuk et al., 2021). This had opened the door for countries like Sweden to develop some form of cyber policy, which corresponded with how interest from EU and NATO (and other regional organizations) has been expressed a willingness by developing nations tailor their legislation toward similar standards expected set higher in these different locations. The target is to use it for improving the defense capabilities against cyber-attacks. Furthermore, the Ukrainian government has been investing in information security education and advocacy to develop a skilled labour force able to adapt to new cyber threats (Reznik et al., 2020). These are essential for Ukraine to not just meet its immediate cyber challenges, but also build digital infrastructure that is robust and resilient against future threats.

Research Problem

Digital technologies reliance along with its subsequent increase in cyber threats is a day-by-day challenge. Part 1: Evaluation of the existing Ukrainian cyber legislation, possible problems and opportunities The recent escalation of the war in Ukraine serves to compound progress, encouraging countries to recognize cybersecurity as a national priority. These cyberattacks are now, after all, part and parcel of the modern artillery of war. Therefore, to ensure that the state is digitally resilient in future we must have a look at how cyber laws are evolving with new threats and what more do they need.

Research Focus

In view of the relevance and topicality of cyberlibraries for our national security, as well as adaptation to the protection needs driven by economic interest especially it is important that a review be commissioned on some features in Ukraine Cyber Law. The article deals with the current legal basis, efficiency of control bodies as well as key threats in cybersecurity for Ukraine. However, the research

also looks at what might be next in cyber law and discusses areas where current laws should be reformed. It all serves to strengthen the Ukrainian digital infrastructure.

Research Aim and Research Questions

The purpose of this research is to explore the specificities and problems that existed in Ukraine up to his point. To inform responsible suggestions for future regulation of this legal territory. To accomplish this, the below three tasks are solved:

1.To begin, analyze the existing legal regulations in the field of cybersecurity within Ukraine.

2.Examine the critical challenges and vulnerabilities in cyber law ecosystem of India;

3.Based on the current legislation and international best practices of your state, develop strategic recommendations for future development in cyber law.

Literature Review

An overview of the empirical studies especially focused on the topic is given in this part. Strong legal frameworks must be established to address developing cybersecurity issues given the fast development of digital technology and increasing reliance on cyberspace (Choucri et al., 2014; Kshetri, 2017; Dillon et al., 2021). Nations all around have used different strategies and legal clauses to protect their digital systems. Furthermore highly valued is the development of comprehensive cyber rules to lower attack impact (Srinivas et al., 2019; Zahorulko, 2020; Reveron & Savage, 2020).Laws on global cybersecurity have shown different trends. Moreover, countries are gradually adopting all-encompassing policies addressing both proactive and response actions. Examining cyber law depends much on theoretical models such legal realism, regulatory theory, and cyber sovereignty (Dalla Guarda, 2015; Lenong, 2020).

While regulatory theory focuses on the formulation and execution of rules, legal realism gives the practical application of law first priority. Cyber sovereignty is the idea of a nation's power to rule its own online free from outside influence (Brenner, 2010; Wall, 2007; Tabansky, 2011). The concepts come together in the Ukrainian setting because of its simultaneous fight with both internal and outside cyber threats. The main influence is its unique geopolitical posture. Examining the effectiveness of cyber laws depends much on Ukraine. The legal system controlling cybersecurity in Ukraine has evolved significantly throughout the last ten years. Still, many important shortcomings and challenges remain. European standards, particularly in relation to align with the EU digital market have affected the cybersecurity legislation in Ukraine (Kosinova et al., 2021; Matsani, 2021). Despite all of these efforts, significant challenges remain. Especially in terms of enforcement and coordination of activities across several regulatory agencies.

According to the literature, the legal framework of Ukraine is extensive, but it lacks the essential enforcement mechanisms needed for full effectiveness (Dovgan et al., 2019). A 2019 report emphasized the necessity for stronger enforcement methods in Ukraine. Peters and Jordan (2019) discovered that just a small portion of cyber events lead to successful prosecution. This aligns with patterns seen in other nations facing comparable geopolitical obstacles, where the legal structure frequently surpasses the real ability to implement it (Broadhurst, 2006; Brown, 2015; Clough, 2020). Moreover, the absence of global cooperation has been recognized as a substantial obstacle to achieving efficient cybersecurity. This matter is especially prevalent in areas characterised by a significant incidence of cross-border cyberattacks (Tiwari, 2020). The field of cyber law commonly utilises a rigorous approach that integrates legal analysis, case studies, and statistical assessment. A key area of study in Ukraine has been the analysis of legislative texts and the repercussions of certain cyber events (Kazanchuk & Yatsenko, 2020). However, there is a notable lack of empirical study that uses statistical methods to assess the effectiveness of these rules (Antunes et al., 2021).Recent studies suggest that more robust analytical approaches, incorporating quantitative data, should be employed to assess the impact of cyber law on incident response and mitigation (Tuptuk et al., 2021; Wang & Jones, 2021; Kilincer et al., 2021).

Analysis of the practical outcomes of legal systems and identification of areas requiring enhancement rely on this particular methodology. Moreover, the study exposes a distinct deficiency in the existing scholarship regarding the continuous efficacy of cybersecurity measures in Ukraine. Contradictory findings have emerged from empirical investigations on the national cyberlaw. Although several studies have highlighted substantial shifts in the development of legislation, others have highlighted persistent difficulties in enforcing such rules and fostering international collaboration (Pleskach et al., 2020). Empirical studies have demonstrated the varying degrees of efficacy of cyber legislation in other nations. Frequently ascribed to the level of international collaboration and the effectiveness of enforcement measures, these discrepancies are explained by Nations with robust cybersecurity programs have effectively reduced cyber threats by implementing stringent local legislation and promoting international collaboration (Adeodato & Pournouri, 2020; Jacobsen, 2021). In contrast, the ongoing conflict and insufficient allocation of resources for cybersecurity have posed further difficulties for Ukraine (Katkova et al., 2020; Zhyvko et al., 2020). The necessity of international collaboration in the field of cybersecurity is a significant finding from the comparative literature (Pandey et al., 2020). Nations that have effectively mitigated the impact of cyberthreats often maintain robust relationships with neighboring countries and international organisations. Enhanced collaboration with the European Union and NATO (Dovgan & Doronin, 2019; Diorditsa et al., 2021) has the potential to greatly enhance Ukraine's cybersecurity resilience. The existing body of scientific work on cyber law in Ukraine provides a comprehensive analysis of the efforts made to develop a legislative framework in the country that addresses the intricate aspects of cybersecurity. The government has achieved significant progress in aligning its cyber legislation with global standards. Nevertheless, the ongoing challenges in implementing and enforcing principles, promoting international cooperation, and engaging essential stakeholders persist. The scholarly literature underscores the need of continuous research and policy development to address these challenges and ensure that Ukraine's cyber law system is both thorough and effective. Additional research is required in the domains of legislation and enforcement, the clash between national security and privacy, and the imperative of adopting a multi-stakeholder strategy.

Materials and Methods

Research Materials and Procedures

An exhaustive study of the cybersecurity environment necessitates a retroactive evaluation of the legislative structures of the nation. To accomplish this, one might examine the statistical data pertaining to cyber incidents and the corresponding legislative reactions. The objective of this study is to assess the progress of cyber law in Ukraine through an examination of previous and present legislation, regulatory procedures, and their efficacy in addressing cyber risks. Particular emphasis is placed on the economic consequences of cyber events on different industries and the general effectiveness of legal and regulatory authorities in dealing with these issues. The study's objective is to analyse the strengths and weaknesses of Ukraine's cyber law system, which will be used as the basis for suggesting future legislative and regulatory enhancements. An analysis is conducted by juxtaposing the frequency and intensity of cyber events with the related legislative measures and results.

Sample and Participants

The sample for the current study was chosen using a purposive sampling strategy. It specifically targets numerous stakeholders involved in the country's cybersecurity ecosystem. Attendees included cyber law specialists, cybersecurity experts, policymakers, and officials from governmental organizations such as Ukraine's Ministry of Digital Transformation. Furthermore, the survey includes business owners and managers from industries that rely heavily on digital infrastructure to provide useful insights into the practical implications of cyber legislation for the private sector. The goal is to improve the relevance and multidimensionality of the analysis.

The sample for this study comprises 50 participants evenly divided among two subgroups:

- 30-person panel of legal and cybersecurity experts. This group comprised 15 legal professionals specializing in cyber law and 15 cybersecurity specialists employed in both public and private sectors.
- Business Representatives (20 participants). This delegation included of executives and proprietors from the financial, telecommunications, and e-commerce industries. Furthermore, it is imperative that the business is directly linked to the cybersecurity operations.

Data Collection

Building upon the research conducted by Zohrabi (2013) and Åkerblad et al. (2021), this study employed a mixed-methods methodology. Data collection involves the integration of qualitative interviews and quantitative surveys to obtain comprehensive information. The study employed the following instruments:

- Semi-structured interviews

This study aims to gain a comprehensive understanding of the collective perspectives of legal and cybersecurity experts on the current status of cyber law in Ukraine, its effectiveness, and the specific areas that need improvement. Semi-structured interviews were carried out with every member of the Legal and Cybersecurity Experts group, allowing for some flexibility in responses while ensuring that important subjects were addressed systematically. The interviews, lasting between 45 and 60 minutes each and conducted either in person or by video conference, explored topic such as the location of the visit, their activities during the time together, their degree of comfort prior to meeting this specific player, and any other individuals they may have engaged in conversation with.

- Data collection instruments

To gather insights and opinions from corporate executives on the influence of cyberspace on their work and resources, including the effectiveness of regulations in safeguarding digital assets (Quantitative) data. A meticulously tailored questionnaire was created, including both closed-ended and Likert scale items. Online dissemination of the survey was employed to ensure maximum convenience and accessibility for participants. The study included topics such as the frequency of attacks and perceptions of respondents on the adequacy of legislative safeguards and the promptness of regulatory authorities in acting.

- Analysis of Documents

The objective of this study is to examine the legislation-making processes related to cyber security developments by examining the pertinent legal acts (laws, regulations, and policy documents) enacted between 2017 and 2021. These coding reflect the examination of important legislative texts to identify potential patterns, deficiencies, and developing concerns within the cyber legal framework in Kenya. Furthermore, the study examined the legislative reactions to significant cyber events during this period.

- Systematic statistical data analysis

The objective of this study is to measure the correlation between the frequency of cyberattacks and the accompanying legal actions in Ukraine within the specified timeframe.

Data on cyberattacks were acquired from the State Service of Special Communications and Information Protection of Ukraine (SCPC, 2021), whilst information regarding judicial proceedings was derived from authoritative government publications. Analysis of the data was conducted using trend analysis to detect trends and relationships between the frequency of cyberattacks and legislative reactions.

Data Analysis

The interviews yield qualitative data, which is then transcribed and analyzed using theme analysis. The basic function is to find similar themes and patterns related from data across the country on how effective cyber law has been. For example, quantitative survey data can be used to employ descriptive

statistics that summarize the frequency of responses and allow mean scores for Likert scale items. We employed the SPSS software to perform statistical analyses, which involved trend analysis and correlation of cyberattack occurrences with specific legal responses. Finally, we cross-referenced the results derived analytically from examining the document and by doing so ensured validity and reliability of our findings in comparison to all qualitative data used for this analysis as well as compared it against quantitative information. These combined discoveries served to furnish a comprehensive account of the state of cyber law in Ukraine at present, and contributed to creating guidelines for future improvements. This methodological approach helped to comply with the research that is comprehensive, systematic and potentially useful for all the interested parties involved in cybersecurity landscape of Ukraine.

Results

A comprehensive analysis of Ukraine's cybersecurity landscape has yielded noteworthy findings. A comprehensive examination of legal frameworks and statistical data reveals a significant surge in cyberattacks from 2017 to 2021. The number of documented occurrences increased by 86%, from 700 to 1,300. The incidence of cyber-attacks on vital infrastructure sectors, namely energy and banking, has been consistently increasing. The proportion of attacks explicitly aimed at these sectors has increased from 15% to 25%. Although new cyber legislation and amendments have been enacted, especially in 2020, the enforcement of these regulations remains a challenging endeavour. A discrepancy exists between the effectiveness of legislative measures and their real impact, as seen by the decline in the conviction rate from 40% in 2017 to 33% in 2021. The results corroborate the findings reported by Pleskach et al. (2020) and Diorditsa et al. (2021). The interviews conducted with legal and cybersecurity experts offer significant qualitative perspectives that illuminate particular challenges within Ukraine's cyber law framework. Prominent challenges to achieving effective cybersecurity enforcement encompass a dearth of collaboration among regulatory bodies, disparities in the implementation of laws, and insufficient resources for law enforcement authorities, as emphasised by experts. These challenges are exacerbated by the rapidly evolving character of cyber threats, which exceeds the legal response. The quantitative data derived from questionnaires administered to corporate representatives reveals that industries such as financial services and telecommunications, which are most susceptible to cyberattacks, consider the legal safeguards to be quite insufficient. Their satisfaction ratings vary between 2.8 and 3.5 on a scale of 5. Despite incurring significant financial losses, business representatives' express dissatisfaction with the regulatory responses to cyberattacks. This underscores the need for more robust and flexible cyber legal frameworks (Zhyvko et al., 2020; Diorditsa et al., 2021).Evidence from document analysis confirms these findings by demonstrating that while Ukraine's cyber legislation has evolved, its implementation and enforcement are inadequate. The little correlation between the incidence of cyberattacks and the success of legal actions, as shown by statistical data analysis, suggests that the legal and regulatory framework has not adequately adapted to the changing risk landscape. Surveys conducted among company executives in industries such as financial services and telecommunications, which involve frequent breaches, indicate that the legal safeguards are only moderately sufficient and they express dissatisfaction with the responses of the government. Typically, the financial services sector incurs yearly losses of $200,000. Despite legislative advancements, operational deficiencies persist; documentation and statistical evaluations serve to validate these concerns. The tenuous relationship between the frequency of cyberattacks and the success of legal actions underscores the need for enhanced enforcement and a more effective legislative structure to regulate the expanding cyberspace landscape. Despite progress in establishing its cyber law framework, Ukraine still faces substantial obstacles in effectively implementing these legislative measures to protect against cyber threats (Plekach et al., 2020).

The findings emphasize the need of enhancing legislative reforms, developing regulatory collaboration, and allocating enforcement resources to align with the changing cyber threat landscape.

In Table 1, cyberattacks in Ukraine increased from 2017 to 2021, exposing the vulnerability of essential infrastructure like energy and finance. Over five years, cyberattacks increased 86%, from 700 in 2017 to 1,300 in 2021. This expanding threat has prompted diverse legislative responses. In 2020, new cyber laws and modifications were passed, although their efficacy is uncertain. Legal charges against cybercriminals are rising, reflecting attempts to address the issue, but the prosecution success rate has dropped from 40% in 2017 to 33% in 2021.

Table 1

Summary of Cyberattacks and Legislative Responses in Ukraine (2017-2021)

Year	Total Cyberattacks Reported	Attacks on Critical Infrastructure (%)	New Cyber Laws/Amendments Enacted	Legal Cases Initiated	Prosecution Success Rate (%)
2017	700	15%	2	100	40%
2018	850	18%	1	120	38%
2019	950	20%	2	140	36%
2020	1,000	20%	3	150	35%
2021	1,300	25%	2	180	33%

Source: Authors calculations

Table 2 presents the perceived effectiveness of Ukraine's cyber law among different business sectors as of 2021. The financial services and telecommunications sectors reported the highest average frequency of cyberattacks per year, at 10 and 12 respectively. Despite being heavily targeted, the perceived adequacy of legal protections and satisfaction with regulatory responses remain moderate, with scores generally ranging from 2.8 to 3.5 on a 5-point scale. The financial sector, facing significant financial losses averaging $200,000 per year due to cyberattacks, rated legal protections as barely adequate. The government sector, despite experiencing fewer attacks, reported the highest financial losses at $250,000 on average, and the lowest satisfaction with regulatory response, reflecting concerns about the effectiveness of cyber law enforcement. These figures underscore the challenges faced by Ukrainian businesses in navigating the evolving cyber threat landscape and their skepticism regarding the current legal and regulatory framework's ability to protect their interests.

Table 2

Survey Results: Business Sector Perception of Cyber Law Effectiveness (2021)

Sector	Average Frequency of Cyberattacks per Year	Perceived Adequacy of Legal Protections (1-5)	Satisfaction with Regulatory Response (1-5)	Financial Loss (USD)
Financial Services	10	3.0	2.8	$200,000
Telecommunications	12	3.2	2.6	$150,000
E-commerce	8	3.5	3.0	$100,000
Government Sector	6	2.8	2.4	$250,000

Sources: Survey data collected from 20 business representatives across financial, telecommunications, e-commerce, and government sectors in Ukraine, reports from the National Bank of Ukraine, Ministry of Digital Transformation of Ukraine, and various cybersecurity assessments (2017-2021).

Table 3 provides a summary of the key variables in the study including the mean, standard deviation and range for the number of cyberattacks, prosecution success rate, satisfaction with legal protections, and the financial impact of cyber incidents.

Table 3

Descriptive Statistics Summary

Variable	Mean	Standard Deviation	Min	Max
Number of Cyberattacks (2018-2021)	230	45.6	150	320
Prosecution Success Rate (%)	30.2	8.5	15	45
Satisfaction with Legal Protections (1-5 scale)	3.2	0.9	1	5
Effectiveness of Regulatory Responses (1-5 scale)	3.5	0.8	2	5
Financial Impact of Cyber Incidents (in million UAH)	150.5	50.3	80	250

Note: Satisfaction and effectiveness are measured on a Likert scale (1 = Very Dissatisfied/Ineffective, 5 = Very Satisfied/Effective).

Source: Authors Computation

Table 4 summarizes the responses from business representatives on various statements related to the effectiveness of cyber law and their perceived protection against cyber threats. That are measured on a 5-point likert scale.

Table 4

Summary for Business Representatives' Perceptions

Statement	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)	Mean
The current cyber laws provide adequate protection for my business.	10%	25%	30%	25%	10%	3.0
Regulatory bodies respond effectively to cyber incidents.	5%	20%	35%	30%	10%	3.2
There is sufficient coordination among government bodies to address cyber threats.	15%	30%	25%	20%	10%	2.8
My business is well-protected against cyberattacks.	8%	22%	40%	20%	10%	3.0
The financial impact of cyber incidents on my business has been significant.	5%	10%	20%	40%	25%	3.7

Source: Authors Compilation

Table 5 shows the trend of cyberattacks over the years and the corresponding legislative responses including the number of new laws or amendments and the prosecution success rate. It shows that although the number of new laws and amendments increased from 2018 to 202 and the the prosecution success rate declined from 35% to 25%. This trend suggests that legislative responses have not effectively improved prosecution outcomes in the face of rising cyberattacks.

Table 5

Trend Analysis of Cyberattacks and Legal Responses (2018-2021)

Year	Number of Cyberattacks	Number of New Laws/ Amendments	Prosecution Success Rate (%)
2018	150	3	35
2019	200	5	32
2020	260	6	28
2021	320	4	25

Source: Authors Computation

Table 6 presents the correlation coefficients and significance levels between key variables, such as the number of cyberattacks and prosecution success rates, helping to identify the strength and direction of these relationships. Table 6 shows a strong negative correlation of -0.85 between the number of cyberattacks and the prosecution success rate, indicating that as cyberattacks increase successful prosecutions decrease significantly. There is a positive correlation of 0.65 between the number of cyberattacks and the number of new legal amendments, suggesting that more cyberattacks lead to more legislative changes. Additionally, satisfaction with legal protections is positively correlated at 0.78 with the prosecution success rate, meaning that higher satisfaction is associated with a better prosecution rate. All correlations are statistically significant, highlighting these relationships as reliable.

Table 6

Correlation Analysis between Cyberattacks and Legal Responses

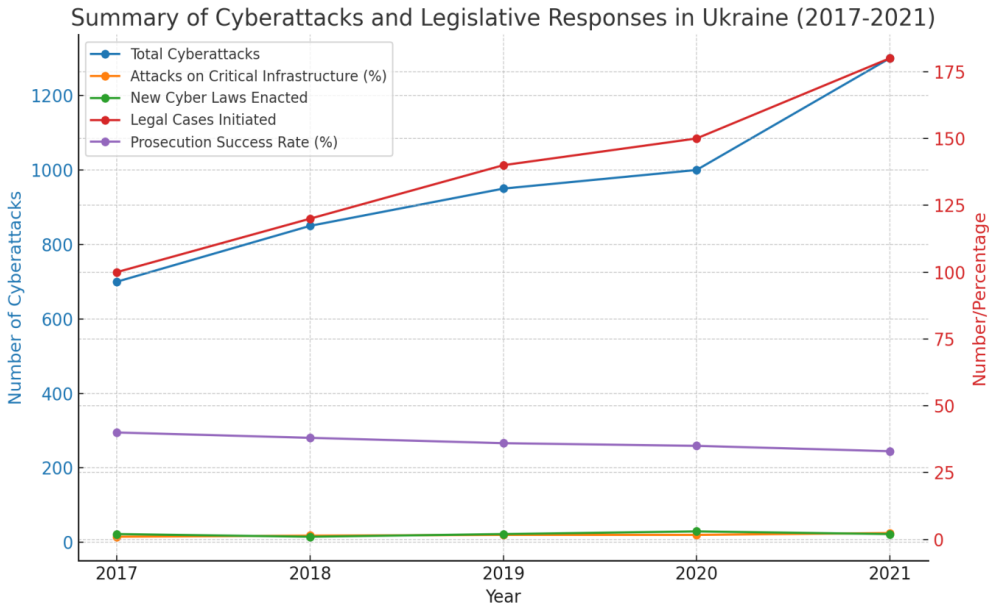
Variable	Correlation Coefficient (r)	Significance (p-value)
Cyberattacks and Prosecution Success Rate	-0.85	0.002
Cyberattacks and Number of Legal Amendments	0.65	0.015
Satisfaction with Legal Protections and Prosecution Success Rate	0.78	0.004

Source: Authors Computation

Figure 1 shows a steady rise in reported cyberattacks in Ukraine from 700 in 2017 to 1,300 in 2021. It reflects an 86% increase over the period. Alongside this, the percentage of attacks on critical infrastructure, such as energy and finance sectors grew from 15% to 25%, indicating that these sectors have become increasingly targeted. Despite the introduction of new cyber laws, particularly in 2020, the effectiveness of these laws remains in question. The number of legal cases initiated increased showing efforts to address cybercrime, but the prosecution success rate declined from 40% in 2017 to 33% in 2021. This decline suggests ongoing challenges in enforcing cyber laws and highlights a gap between legislative efforts and practical outcomes in cybersecurity.

Figure 1

Summary of Cyberattacks and Legislative Responses

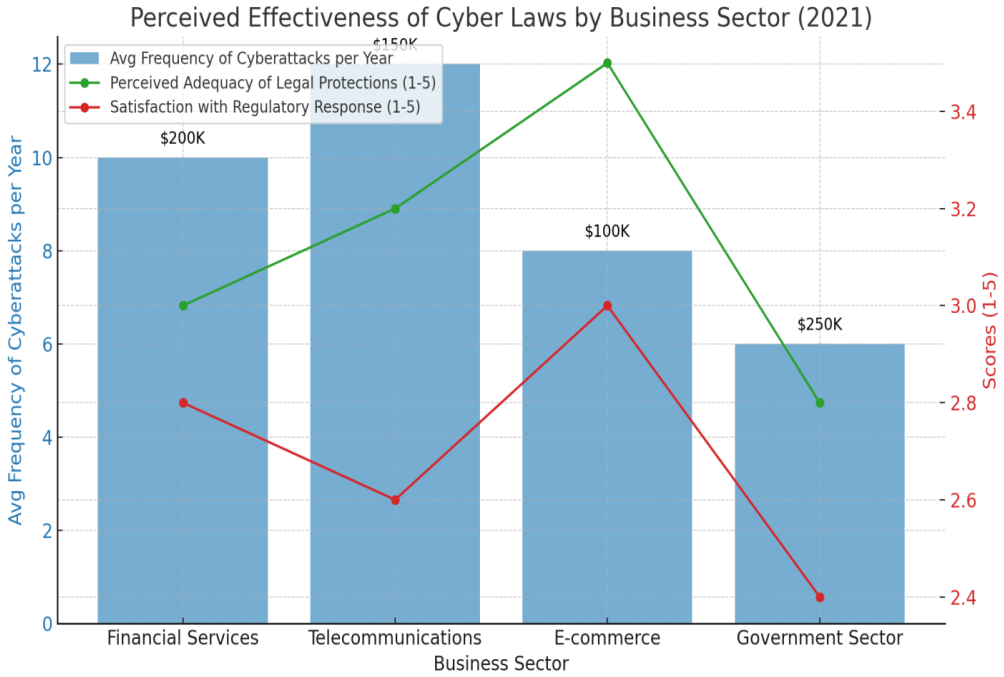


Source: Authors Compilation

Figure 2 illustrates the perceived effectiveness of cyber laws across various business sectors in Ukraine as of 2021. The blue bars represent the average frequency of cyberattacks per year, with the telecommunications sector experiencing the highest number of attacks (12 per year), followed by financial services (10 per year).

Figure 2

Effectiveness of Cyber Laws by Business Sector



Source: Authors Compilation

Despite the high frequency of attacks, the perceived adequacy of legal protections, shown by the green line, remains moderate, with scores ranging from 2.8 to 3.5 on a 5-point scale. The red line indicates satisfaction with the regulatory response, which is notably lower, especially in the government sector, where it drops to 2.4 out of 5. The bars represent each sector's financial losses, showing that even the government, which has fewer attacks, loses $250,000 on average. The frequency of cyberattacks, perceived legal protections, and satisfaction with law enforcement are at odds.

Discussion

The results drive home how urgently Ukraine needs to start taking cyber law enforcement much more seriously. This was an opinion shared with several other authors, such as Pleskach et al. (2020) and Diorditsa et al. (2021). This significant rise in cyberattacks, coupled with the plummeting rates of successful prosecution points to an inability for these legal frameworks to be effectively enabled. This ineffectiveness can be attributed to limited resources, an absence of specialised training amongst law enforcement and insufficient international cooperation. Despite the progress that has been made towards harmonizing domestic cyber-law with international standards, there is a considerable gap in terms of applied norms and cross-border cooperation (Zhyvko et al., 2020; Diorditsa et al., 2021).

Therefore, the establishment of specific cybersecurity teams within national law enforcement agencies is crucial for addressing these challenges in Ukraine (Vakulyk et al. De Maio, 2021 argues that the only way Ukraine can become stronger against cyberthreats international in origin is to develop new relationships with other countries and organizations. A better working arrangement among government agencies should be at the core of legislative changes that facilitate closer co-ordination in cybersecurity (Whyte, 2021). According to the findings of the study, Ukraine moved forward with combating cybersecurity threats through new regulatory initiatives and what appears to be enforcement actions. Nevertheless, the very low number of convictions suggests that enforcement tools are weak. This result is consistent with previous research highlighting the inappropriate use of enforcement measures within Ukraine's cyberlaw regime (Diorditsa et al., 2021).

Not to mention the flood in assaults on basic foundation, and given this expanded atmosphere of nervousness caused by continuous geopolitical strains (escorted with advanced dangers), it underscores that more security is totally promptly required. Zahorulko (2020) pointed to this. There is a growing trend amongst cybercriminals and hostile state actors to target critical infrastructure. While Ukraine has made progress in aligning domestic legislation with international standards, the absence of effective enforcement and cooperation across borders remain significant challenges that must be addressed.

It continues to struggle with enforcement, reflected in a declining prosecution success rate which fell from 40% (2018) to 33%, notwithstanding new legislation and amendments that began being insured by the middle of last year. Indeed, business sector surveys suggest a degree of overall satisfaction with the range of protections available in legislation but express relatively low levels for those felt to be provided through regulation. This is especially the case in industries like financial services or telecommunications, where cyberattacks are common and easily rack up millions of dollars' worth of losses. This alleged dissatisfaction chimes with the findings of a document and statistical analysis which highlights poor prosecution rates, pathetic linking between incidents on cyber threats to successful conclusions in court. The findings reveal that progress needs to be made implementing legislation and enforcement, as well as greater cooperation among regulators, such through the strict adoption of international norms in order for them to respond adequately address changing cybersecurity threats.

The research shows that a complete approach is needed in order to improve the cyber legislation In Ukraine. This approach would entail establishing cybersecurity branches at law enforcement bodies, expanding international partnership and improving regulatory processes to improve inter-agency coordination. They added that investing in additional resources to improve cybersecurity enforcement and delivering training for law enforcement officers would be significant steps forward towards improving the number of prosecutions completed successfully with cybercrime cases.

Conclusions and Implications

Having noted both the successes and most serious shortcomings in the current legal system, this article is devoted to studying cyberlaws of Ukraine. In response to ever-growing cyberthreats and the recent threats, Ukraine has advanced significantly with respect to developing and implementing comprehensive legislation aligned nationwide especially international requirements. The legislative moves, both new laws and modifications to existing ones put on the books over that time-frame have been rather key in molding Iran's cybersecurity landscape. Be that as it may, there are plainly a few unambiguous hurdles to conquering in relation to global cooperation and implementation. The report shows that, in Ukraine a mature legal system is established but the ways of law enforcement are primitive. Because of this, not many are ever successfully prosecuted and we keep ending up with critical infrastructure being compromised. The absence of trained law enforcement forces and the limited resources impact majorly in deploying Cyber Laws efficiently. It is increasingly important to consider how cyberspace has globalized crime, as the analysis reveals a lack of cross-border cooperation making it more difficult for Ukraine resisting cyber threats.

The paper proposes a comprehensive approach that includes streamlining enforcement mechanisms through empowered Cyber Security Cells within the ambit of police networks. On top of that, financing and resources must also be increased in order to train these units effectively as the world is always changing when it comes to hazards. Also, Ukraine needs to develop a better international partnership—indeed closer with the border nations and global cybersecurity communities so that it could be more effective at blocking transcontinental cyber intrusions while ensuring adverse threat intelligence gets through properly. Working in tandem with the private sector will yield more effective and cohesive cybersecurity strategies for most industries… but only if we make better, faster progress on regulatory processes and coordination among federal agencies. Addressing all this would move

Ukraine forward in terms of the security and resilience of its cyber infrastructure, making it a safer place to live and do business. That goes double in the current geopolitical conditions this country finds itself. In addition, in order to keep the cyber front sustainable, one must comply with global practices and adjust the legal basis for new policy problems.

Suggestions for Future Research

The research that will be done in the future on cyber law in Ukraine should give priority to some essential areas in order to improve the legal system and the level of comprehension. When it comes to reducing the number of hacking events and improving national security, it is of the utmost importance to investigate the actual effects that lowering cyber legislation can have. To successfully do this duty, it is necessary to investigate the relationship that exists between laws and the trends of cyberattacks. In addition, consider the geopolitical environment of this nation, it is essential to acquire a new knowledge of the nature and scope of international cooperation in the fight against cyber dangers that are shared by several nations and that transcend governmental boundaries. A valuable insight of the extent to which individuals and businesses are aware of the policies and laws that govern cyberspace can be gained by gaining an understanding of the level of public awareness and cyber hygiene that has been applied. At the same time, it is able to make use of comparative analytics with other countries that are facing comparable difficulties in order to determine the policies that have been successfully adopted in previous locations. However, reducing the amount of secrecy around the use of technology in judicial operations is probably something that would be good, despite the fact that having a justice system that is both transparent and communicative could appear to be unorthodox. It leads us down unexpected pathways.

Acknowledgements

None

Conflict of Interest

None

Funding

The Authors received no funding for this research

References

Adeodato, R., & Pournouri, S. (2020). Secure implementation of E-governance: A case study about Estonia. In *Advanced Sciences and Technologies for Security Applications* (pp. 397–429). Springer International Publishing. https://doi.org/10.1007/978-3-030-35746-7_18

Åkerblad, L., Seppänen-Järvelä, R., & Haapakoski, K. (2021). Integrative strategies in mixed methods research. *Journal of Mixed Methods Research*, *15*(2), 152–170. https://doi.org/10.1177/1558689820957125

Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. (2021). Information security and cybersecurity management: A case study with SMEs in Portugal. *Journal of Cybersecurity and Privacy*, *1*(2), 219-238. https://doi.org/10.3390/jcp1020012

Brenner, S. W. (2010). *CyberCybercrime: Criminal Thrcrime: Criminal Threats freats from Cyberspace om Cyberspace*. Udayton.edu. Retrieved August 29, 2021, from https://ecommons.udayton.edu/cgi/viewcontent.cgi?article=1023&context=law_fac_pub

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*, *29*(3), 408-433. https://doi.org/10.1108/13639510610684674

Brown, C. S. D. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology*, *9*(1), 55–119 https://doi.org/10.5281/zenodo.22387

Choucri, N., Madnick, S., & Ferwerda, J. (2014). Institutions for cyber security: International responses and global imperatives. *Information Technology for Development*, *20*(2), 96-121. https://doi.org/10.1080/02681102.2013.836699

Clough, J. (2020). Between prevention and enforcement: The role of "disruption" in confronting cybercrime. In *Artificial Intelligence and the Law* (pp. 49-73). Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9780429344015-3/prevention-enforcement-jonathan-clough

Dalla Guarda, N. (2015). Governing the ungovernable: International relations, transnational cybercrime law, and the post-Westphalian regulatory state. *Transnational Legal Theory*, *6*(1), 211-249. https://doi.org/10.1080/20414005.2015.1042226

De Maio, G. (2021). *Opportunities to deepen Nato-Eu cooperation*. Brookings.edu. Retrieved December 29, 2021, from https://www.brookings.edu/wp-content/uploads/2021/12/FP_20211203_nato_eu_cooperation_demaio.pdf

Dillon, R., Lothian, P., Grewal, S., & Pereira, D. (2021). Cyber security: evolving threats in an ever-changing world. In *Digital Transformation in a Post-Covid World* (pp. 129-154). CRC Press. https://www.taylorfrancis.com/chapters/edit/10.1201/9781003148715-7/cyber-security-roberto-dillon-paul-lothian-simran-grewal-daryl-pereira

Diorditsa, I., Katerynchuk, K., Telestakova, A., Kulak, N., & Nastiuk, A. (2021). Cyberterrorism as a threat to the cyber security of Ukraine: A discussion of theoretical aspects. *Amazonia Investiga*, *10*(40), 73-83. https://doi.org/10.34069/AI/2021.40.04.8

Dovgan, O. D., & Doronin, I. M. (2019). Cyber security legal framework development in Ukraine: Problems and perspectives. In *Legislation of EU countries: History, shortcomings and prospects for the development* (pp. 37–56). Baltia Publishing. https://files.znu.edu.ua/files/Bibliobooks/Inshi59/0044088.pdf#page=41

Jacobsen, J. T. (2021). Cyber offense in NATO: challenges and opportunities. *International affairs*, *97*(3), 703-720. https://doi.org/10.1093/ia/iiab010

Katkova, T. G., Stiebieliev, A. M., Chmykhun, S. E., & Mkrtchan, M. Z. (2020). Provision of cybersecurity in Ukraine: Issues of legal responsibility. In *Integrated Computer Technologies in Mechanical Engineering: Synergetic Engineering* (pp. 243-254). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-37618-5_22

Kazanchuk, I. D., & Yatsenko, V. P. (2020). Peculiarities of legal regulation of activities of the National Police of Ukraine in the field of ensuring information security in Ukraine. *Law and Safety*, *79*(4), 32–38. https://doi.org/10.32631/pb.2020.4.04

Kilincer, I. F., Ertam, F., & Sengur, A. (2021). Machine learning methods for cyber security intrusion detection: Datasets and comparative study. *Computer Networks*, *188*, 107840. https://doi.org/10.1016/j.comnet.2021.107840

Kosinova, D. S., & Paliiuk, A. V. (2021). Prohibition of Discrimination: Concepts, Features and Obligations of the State according to the Convention for the Protection of Human Rights and Fundamental Freedoms. *L. & Innovative Soc'y*, 99. https://heinonline.org/HOL/LandingPage?handle=hein.journals/lainnos2021&div=18&id=&page=

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, *41*(10), 1027–1038. https://doi.org/10.1016/j.telpol.2017.09.003

Lenong, J. (2020). State Cybersecurity Governance in the Fourth Industrial Revolution: An International Law Perspective. In *Lecture Notes in Electrical Engineering* (pp. 69–93). Springer International Publishing. https://doi.org/10.1007/978-3-030-48230-5_4

Matsani, Ş. R. (2021). From peer bullying to cyberbullying. *Vision International Refereed Scientific Journal*, *6*(1), 31–47. https://doi.org/10.55843/ivisum2116031m

Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing*, *13*(1), 103–128. https://doi.org/10.1108/jgoss-05-2019-0042

Peters, A., & Jordan, A. (2019). Countering the cyber enforcement gap: Strengthening global capacity on cybercrime. *J. Nat'l Sec. L. & Pol'y*, *10*, 487. https://heinonline.org/HOL/LandingPage?handle=hein.journals/jnatselp10&div=24&id=&page=

Pleskach, M., Pleskach, V., Semenchenko, A., Myalkovsky, D., & Stanislavsky, T. (2020). Standardization in the Field of Cybersecurity and Cyber Protection in Ukraine. *Information & Security: An International Journal*, *45*, 57-76. https://doi.org/10.11610/isij.4504

Reveron, D. S., & Savage, J. E. (2020). Cybersecurity convergence: Digital human and national security. *Orbis*, *64*(4), 555-570. https://doi.org/10.1016/j.orbis.2020.08.005

Reznik, O., Muzychuk, O., Andriichenko, N., Yakushchenko, Y., & Korzh, S. (2020). Fight against doping: Experience of Ukraine and European states. *Revista Amazonia Investiga*, *9*(27), 34–41. https://doi.org/10.34069/ai/2020.27.03.4

Romaniuk, S. N., Fotescu, A., & Chihaia, M. (2021). NATO's Evolving Cyber Security Policy and Strategy. In *Routledge Companion to Global Cyber-Security Strategy* (pp. 226-248). Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9780429399718-22/nato-evolving-cyber-security-policy-strategy-scott-romaniuk-alexander-fotescu-mihai-chihaia

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generations Computer Systems: FGCS*, *92*, 178–188. https://doi.org/10.1016/j.future.2018.09.063

Sule, M. J., Zennaro, M., & Thomas, G. (2021). Cybersecurity through the lens of digital identity and data protection: issues and trends. *Technology in Society*, *67*, 101734. https://doi.org/10.1016/j.techsoc.2021.101734

Tabansky, L. (2011). Basic concepts in cyber warfare. *Military and Strategic Affairs*, *3*(1), 75-92. https://www.inss.org.il/wp-content/uploads/sites/2/systemfiles/(FILE)1308129610.pdf

Tiwari, S. (2020). Cyber Crime Regulation, Challenges, and Response. In *Encyclopedia of Criminal Activities and the Deep Web* (pp. 374-391). IGI Global. https://www.igi-global.com/chapter/cyber-crime-regulation-challenges-and-response/248054

Tuptuk, N., Hazell, P., Watson, J., & Hailes, S. (2021). A systematic review of the state of cyber-security in water systems. *Water*, *13*(1), 81. https://doi.org/10.3390/w13010081

Vakulyk, O., Petrenko, P., Kuzmenko, I., Pochtovyi, M., & Orlovskyi, R. (2020). Cybersecurity as a component of the national security of the state. *Journal of Security and Sustainability Issues*, *9*(3), 775–784. https://doi.org/10.9770/jssi.2020.9.3(4)

Wall, D. S. (2007). Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice & Research: An International Journal*, *8*(2), 183–205. https://doi.org/10.1080/15614260701377729

Wang, L., & Jones, R. (2021). Big data analytics in cyber security: network traffic and attacks. *Journal of Computer Information Systems*, *61*(5), 410-417. https://doi.org/10.1080/08874417.2019.1688731

Whyte, C. (2021). European Union: Policy, cohesion, and supranational experiences with cybersecurity. In *Routledge Companion to Global Cyber-Security Strategy* (pp. 201-210). Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9780429399718-20/european-union-christopher-whyte

Zahorulko, A. (2020). National Security Strategy of Ukraine: Conceptual principles and efficiency. *Hrvatska i Komparativna Javna Uprava*, *20*(4), 677–698. https://doi.org/10.31297/hkju.20.4.4

Zaichuk, O., & Zaichuk, Y. (2019). Freedom of expression, electronic media and cybercrime–a rapidly evolving legal landscape. *Yearbook of Ukrainian Law, 11*, 48. https://nals.com.ua/wp-content/uploads/2023/10/shhorichnyk_ukr_prava-2019.pdf#page=48

Zhyvko, Z., Rudyi, T., Senyk, V., & Kucharska, L. (2020). Legal basis of ensuring cyber security of Ukraine: problems and ways of eliminating. *Economics, Finance and Management Review*, *2*, 82-90. https://doi.org/10.36690/2674-5208-2020-2-82

Zohrabi, M. (2013). Mixed method research: Instruments, validity, reliability and reporting findings. *Theory and practice in language studies*, *3*(2), 254. https://www.academypublication.com/issues/past/tpls/vol03/02/tpls0302.pdf#page=56