NUOVA ANTOLOGIA MILITARE
RIVISTA INTERDISCIPLINARE DELLA SOCIETÀ ITALIANA DI STORIA MILITARE

NAM Studies & Documents

Special Dossier October 2025
Ukraine Military and Wartime Law

Edited by Ganna Sobko

Società Italiana di Storia Militare

Public administration reforms under martial law in Ukraine: International experience of adapting to hybrid threats

by Oleksandr Kurilets[1], Kateryna Manuilova[2], Oleksii Malovatskyi[3], Olena Pavlova[4]

Abstract. The aim of the study is to analyse the transformations of public administration in Ukraine in wartime under the influence of hybrid cyber threats, taking into account international experience in adapting public authorities to new challenges. The relevance of the study is determined by the surge in cyberattacks against public authorities in Ukraine in 2022-2023, which demonstrated the vulnerability of digital infrastructure and the limitations of interagency coordination. The research methodology is based on systemic and comparative legal approaches, typology of hybrid threats and political effects, and empirical analysis of cyberattacks in 2021-2023. Data visualisation tools and scenario analysis of specific incidents were used. The comparative analysis of international cyber defence models in the USA, Israel, Poland, Ukraine was used to verify the results. As a result, three types of new hybrid threats are identified. Moreover, the authors' model of cascading instability is suggested which demonstrates how cyber threats can transform into political destabilisation. In addition, a classification of the political effects of cyberattacks is offered. International experience shows that effective cyber deterrence models are based on centralised coordination, public-private partnerships, and preventive threat management. The conclusions emphasise the

1 PhD Student, Department of Theory and History of the State and Law «KROK» University, 03113, 30-32 Tabirna Str., Kyiv, Ukraine. https://orcid.org/0009-0005-7855-5297.

2 Doctor of Public Administration, Associate Professor, Department of Public Administration and Regionalism, Educational and Scientific Institute of Public Service and Administration, Odesa Polytechnic National University, 65044, 1 Shevchenko Ave., Odesa, Ukraine. https://orcid.org/0000-0002-0721-7232.

3 PhD in Law, Post-Doctoral Researcher, Section of International Private Law, Academician F.H. Burchak Scientific-Research Institute of Private Law and Entrepreneurship of the National Academy of Legal Science of Ukraine, 03150, 11 Kazymyr Malevych Str., Kyiv, Ukraine. https://orcid.org/0000-0002-6370-8028.

4 PhD in Sociology, Associate Professor, Department of Psychology, Pedagogy and Social Sciences, State Tax University, 08200, 31 Universitetska Str., Irpin, Ukraine. https://orcid.org/0000-0002-3624-2525.

NAM, Anno 6 – Special Dossier
DOI: 10.36158/97912566922177
Ottobre 2025

need to rethink Ukraine's cyber strategy from a technocratic document to an integrated component of public policy aimed at strengthening digital sovereignty, institutional resilience, and post-war recovery.

Keywords: public administration; war; cybersecurity, hybrid threats; cascading instability; sovereignty.

1. Introduction

Hybrid warfare is a serious challenge for public administration in the 21st century. It transforms perceptions of security, sovereignty, and administrative efficiency, going far beyond traditional military operations. Cyberspace, information influence, economic blackmail, and stability undermining affect the political stability and social security of states (Zvezdova & Vakalyuk, 2022). In this context, the state ceases to be an exclusively political and administrative structure and becomes a system that functions in interaction with global digital flows, geopolitical risks, and unstable network threats (Yagunov et al., 2023).

The experience of recent decades shows that the effectiveness of public administration in conditions of hybrid aggression is determined by the ability to integrate institutional response mechanisms with technological solutions in cyber defence and information security. Interagency coordination, strategic communication, and the participation of the private sector and civil society are particularly important. As a state experiencing protracted hybrid aggression, Ukraine is a unique case for researching public administration effectiveness in a new type of war (Okunovska & Prymush, 2024). Since 24 February 2022, the high rate of attacks on the digital infrastructure of state authorities, the paralysis of critical services, the spread of disinformation campaigns, and the destruction of institutional coordination have highlighted the need for a radical update of approaches to public administration.

However, the domestic regulatory model of cyber defence proved to be unprepared to counter multi-level threats. The lack of interagency coordination, the low level of readiness of regional infrastructure, and the limitations of the regulatory framework, and the insufficient transparency of response processes created conditions for the consistent destabilisation of public administration. Meanwhile, the experience of the USA, Israel, and Poland demonstrates the effectiveness

of integrated cyber deterrence strategies that combine institutional centralisation, preventive thinking, and active participation of the private and civil sectors. This creates conditions for cascading destabilisation of management processes through targeted cyber pressure. At the same time, global institutions such as NATO and the European Union emphasise the need to develop resilience-based governance models that simultaneously take into account military, cyber and information threats (Cherep et al., 2025).

Despite the growing number of studies of hybrid warfare and cybersecurity, most of them address these issues from the perspective of military science, informatics, or law enforcement (Bondarenko et al., 2025). However, there are gaps in research on the relationship between hybrid cyber threats and the effectiveness of public administration, institutional coordination in crisis situations, and models of public authority adaptation to new types of threats. The aim of the study is to analyse the transformations of public administration in Ukraine in wartime under the influence of hybrid cyber threats, taking into account international experience in adapting public authorities to new challenges. In this regard, the research questions of what are the typologies of the latest threats in the system of public administration, how would the effectiveness of response change if Ukraine had a specialised cyber incident crisis management centre, and how the basic functions of the state are transformed in conditions of permanent digital pressure are raised. Within this aim and research questions, the following objectives are set:

- to develop a typology of hybrid threats that arise in cyberspace during wartime;
- to suggest a hypothetical model of interaction between cyber threats and political governance;
- to compare cyber deterrence models in the United States, Israel, Poland, and Ukraine;
- to assess the effectiveness of Ukraine's cybersecurity strategy in the context of restoring governance capacity in wartime.

The novelty of the study lies in the fact that a comprehensive analysis of the impact of hybrid cyber threats on public administration in Ukraine in wartime is carried out on the basis of empirical data. Moreover, a classification of threat types and political effects is developed. A hypothetical model of cascading destabilisation of management processes through cyber influence is proposed, and structural limitations of the Ukrainian cyber defence system are identified in comparison with advanced international models.

2. Methodological framework

The methodology is based on the interdisciplinary approaches that allow for a comprehensive understanding of the transformations of the public administration system during hybrid warfare. Given the interaction of cyberspace, institutional coordination, and political processes, several research methods were applied. In particular, a systematic method enabled the analysis of public administration as a complex socio-political system functioning in conditions of multidimensional external threats, including cyberattacks. It made it possible to identify key structural nodes (institutional, informational, and procedural).

The comparative legal analysis involved the study of cyber strategies and regulatory models in the United States, Israel, Poland, and Ukraine. The criteria for comparison were the degree of centralisation, the availability of crisis protocols, the interaction with the private sector, and the speed of response. The typological method was used to classify hybrid cyber threats and political effects. This method helped to construct a logical matrix of the impact of cyber incidents on management processes. The empirical analysis is based on open sources (CERT-UA reports, State Service of Special Communications and Information Protection of Ukraine (SSSCIP) reports, analytical publications, government communications).

Quantitative data on cyberattacks in 2021-2023 was collected, presented in the form of time series, a heat map of the most vulnerable points, and systematised in an incident table. An analytical database was created with over 50 cases of attacks on state structures, coded by type of threat, target, duration, institutional response, and political consequences. Verification of the authors' model of cascading instability was carried out by comparing the typology of attacks with the responses of state bodies. A scenario analysis of three incidents (the attack on Diia, the attack on the Ministry of Defence, and the hacking of interagency channels) was conducted, which demonstrated how the absence of a single coordination centre intensifies political and administrative fragmentation.

A modelling method was used to model a hypothetical situation: how would the effectiveness of response change if Ukraine had a specialised cyber incident crisis management centre? The model was developed by analogy with the structures of CISA (USA) and INCD (Israel), considering Ukrainian realities. Cross-verification of data was carried out by comparing official reports with me-

dia reports, independent analytical platforms, and public statements by government representatives. Individual elements were verified through expert assessments in open sources. The study of specific cases of cyberattacks on Ukrainian government structures (2022-2023), such as attacks on the Diia portal, the Ministry of Defence of Ukraine, and the Security Service of Ukraine (SSU), was used to illustrate the identified typologies and verify the suggested model. The study also uses examples of rapid response in other countries (INCD, CISA, Cyber Command) as a reference for assessing the effectiveness of the Ukrainian case.

Thus, the combination of these methods allowed for a comprehensive study of the impact of hybrid cyber threats on Ukraine's public administration system in wartime. The methods used facilitated analytical depth, and the constructed model of cascading instability visualised the complex interrelationships between digital attacks and political processes. Such methodological tools open up opportunities for further research in the field of adaptive public administration under conditions of hybrid threats.

3. Results and Discussion

3.1. Empirical observations: time series of attacks and heatmap of vulnerable points

According to official data, 1,237 incidents related to cyberattacks on Ukrainian government structures were recorded in 2021. With the start of the full-scale Russian invasion in 2022, the number of attacks doubled to 2,474. In 2023, 3,198 incidents were recorded, which is 29,3% more than in 2022. These data indicate a consistent escalation of cyber war against Ukraine, accompanying military actions on the frontline. The highest peaks of malicious activity were recorded in February 2022 (invasion), October 2022 (missile strikes on critical infrastructure), and January and June 2023 (Ukrainian army taking the initiative on the frontline) (State Service of Special Communications and Information Protection of Ukraine, 2024a).

The analysis of quarterly and annual reports from the SSSCIP, the CERT-UA team, and official government communications for 2022-2023 confirms a steady increase in the intensity of cyberattacks and a gradual sophistication of adversary tactics. At the end of 2023, CERT-UA reported 2,543 cyber incidents, reflecting

an increase in the number of intrusion attempts and an improvement in the ability to detect and document them (State Service of Special Communications and Information Protection of Ukraine, 2024b). Moreover, in Q4 2023, state monitoring tools processed about 1,4 billion events, indicating noise from attacks and attempts to probe security perimeters (State Cyber Protection Centre State Special Communications, 2024).

Furthermore, the timeline of attacks shows the synchronisation of cyberattacks with key political or military events. For instance, in January-March 2022, there was a wave of attacks on government resources (defacements, DDoS), which accompanied the start of a full-scale invasion and was aimed at undermining the availability of government websites and services (Polityuk, 2022; Ministry of National Defence of the Republic of Poland, 2022). In October-November 2022, there was a combination of cyberattacks on energy facilities and missile strikes (attempts to influence ICS/SCADA and energy networks) (Greenberg, 2023). Moreover, throughout 2023, phishing and espionage campaigns against the public sector (UAC group cluster, spear-phishing) were frequent, accompanied by periodic waves of DDoS attacks against e-government services (Cert-EU, 2023; Cyber Incident Response Operations Centre, 2024). This tendency indicates a high level of coordination of cyberattacks with other forms of hybrid influence, such as disinformation campaigns, in order to influence public sentiment and management processes. They are part of the enemy's strategic plan to destabilise Ukraine in the areas of governance, information space, and the economy.

The types of attacks varied. Thus, approximately 47% were DDoS attacks aimed at disabling government portals; 32% were attempts at phishing or compromising the accounts of officials; 11% were malware attacks (programmes such as WhisperGate and HermeticWiper); and 10% were attacks on cloud environments or attempts to interfere with internal IT infrastructures. In terms of their structure, in 2022-2023, these incidents were concentrated in the sectors of public administration, security, defence, telecommunications, and energy. Numerous malicious activities were also recorded against financial, logistics, and media resources as part of broader information operations (National Cybersecurity Coordination Centre, 2024). Some waves targeted judicial and notary authorities, with the aim of complicating transactions and legal procedures during wartime (National Cybersecurity Coordination Centre, 2023). However, it is concerning that some of the cyberattacks went undetected for a long time. According to open data, at least

8% of attacks detected in 2023 lasted more than 48 hours before being detected, indicating limitations in the early detection and response capabilities operations (National Cybersecurity Coordination Centre, 2024). In this regard, the spatial heat map of vulnerable points has a two-tiered structure (Table 1).

Table 1. Spatial heat map of vulnerable points

Target of attack	Type of services/ infrastructure	Number of incidents (2023)	Attack aim
Ministry of Digital Transformation of Ukraine and digital service platforms	E-government, digital identification, public services	**580+**	Massive DDoS attacks, defacements, attempts to compromise user accounts
State Tax Service of Ukraine and financial data exchange platforms	Financial and administrative services, tax registers	**470**	Phishing, espionage campaigns, interference with transaction data
Ministry of Defence of Ukraine and military command systems	C2 systems, military communications, secure networks	**410+**	Attempts to infiltrate military networks, targeted phishing attacks
Central Election Commission of Ukraine and local government bodies	Electoral registers, municipal services, local domains	**~300**	Website defacement, attempts to compromise local accounts
Prozorro, eHealth and other digital platforms	Public procurement, healthcare, critical databases	**250+**	Attacks on supply chains, access to personal and commercial data

Source: Cert-EU (2023).

The first tier consists of central government bodies and national registries in Kyiv. In this case, cyberattacks target nodes with a high concentration of critical services and interdepartmental integrations. The second tier is regional and local authorities and critical infrastructure nodes (telecommunications and energy), including on the frontline and border areas. As a result, vulnerabilities are aggravated by physical threats, staff turnover, and uneven defence capabilities. The early period of the war saw massive compromises of local and regional government websites, which evolved into more targeted espionage campaigns against key institutions (Canadian Centre for Cyber Security, 2022).

3.2. Typology of hybrid threats in public administration

In contemporary wartime, Ukraine confronts not only direct military threats but also a complex set of hybrid challenges targeting its political and administrative capacity. Hybrid warfare combines military, economic, informational, social and technological factors (Voloshchuk et al., 2025). Since cyberattacks take place in digital space, identifying the aggressor is complicated, which in turn limits the applicability of traditional international legal response mechanisms. Therefore, it is necessary to rethink the conceptual foundations of public administration.

The asymmetry is an important element of hybrid threats, meaning that relatively insignificant resources directed at disinformation campaigns or cyberattacks can cause damage comparable to the consequences of large-scale military operations (Legenkyi et al., 2025). Meanwhile, states have become dependent on digital infrastructure and e-governance as resource management systems, coordination of military and civilian structures, and effective communication with the population are based on digital technologies, making them a priority target for the enemy. Apart from that, a distinctive feature of hybrid threats is their systemic nature. In most cases, they do not function in isolation but form a complex political shock effect (Stokel-Walker, 2022). This means that simultaneous pressure on infrastructure, the information space, and administrative institutions creates a synergistic effect. As a result, even a technically prepared and formally protected state may be unable to restore stability quickly.

The cumulative effect is another characteristic feature of hybrid threats. Thus, cyberattacks are combined with information manipulation, economic sabotage, and the provocation of social tension (Yakymchuk, 2019). This creates a crisis of confidence because society begins to doubt the ability of state institutions to ensure a basic level of security and stability. Moreover, the cross-border nature of hybrid warfare is an additional complicating factor as cyberattacks are often coordinated from outside the state, using the infrastructure of third countries or global digital platforms (Simons et al., 2020). As a result, hybrid threats go beyond the scope of national security alone and require international cooperation and the adaptation of state institutions to new realities.

Hence, the analysis of contemporary hybrid threats shows that their impact on public administration in wartime is observed in three key areas: technological vulnerability of digital infrastructure, manipulative pressure on public consciousness, and organisational destabilisation of public authorities. On the basis of these

characteristics, a new typology of hybrid threats in the digital age is developed. They are divided into three interrelated types: infrastructure threats, information and psychological influences, institutional and network attacks, and systemic effects (Table 2).

Table 2. Typology of hybrid threats in public administration in wartime

Type of hybrid threat	Content and target	Key tools and methods	Effects on public administration	Examples
Infrastructure threats	Disruption of Ukraine's digital and administrative infrastructure, blocking of basic services	Cyberattacks on critical government services, DDoS attacks, malicious software injections, unauthorised access attempts, data substitution	Paralysis of access to e-services, decline in trust in the digital state, additional burden on administrators during wartime	In 2023, more than 3,198 attacks on the digital infrastructure of state bodies were recorded (29% more than in 2022).
Information and psychological influences	Undermining the legitimacy of the authorities, creating an atmosphere of chaos and panic	Disinformation and propaganda campaigns, deepfake imitations of speeches, targeted attacks on social networks	Decline in public trust, destabilisation of the political environment, creation of an image of incompetent administration	Fake messages on behalf of the Ministry of Defence of Ukraine in 2022-2023; cyberattacks on media resources
Institutional and network attacks	Violation of interdepartmental coordination and decision-making process	Disabling government communication channels, infecting internal systems, imitating official communications	Delays in response, reduced effectiveness of strategy implementation, undermining of trust between institutions	Attacks on the internal systems of the Cabinet of Ministers of Ukraine, the SSU, and SSSCIP in early 2023
Systemic effects	Combination of several types of threats that reinforce each other	A combination of infrastructure attacks, information manipulation, and network destabilisation	Political shock, paralysis of governance, and intensification of internal crises	Estonia (2007, cyberattacks), the United States (2016, election interference), Israel (2021, attacks on government services)

Source: compiled by the authors

This typology demonstrates that the key vulnerability occurs at the intersection of three interrelated dimensions: technical, informational, and institutional. In other words, infrastructure attacks undermine the technical basis of public administration, limiting the state's ability to provide administrative and social services. Information and psychological influences target public consciousness and political trust, creating conditions for the delegitimisation of authority. Institutional and network attacks destroy the mechanisms of interagency coordination.

3.3. Evaluating cyber defence models from the USA, Israel, Poland, and Ukraine

To identify potential directions for reforming Ukraine's cyber strategy, it is useful to compare the Ukrainian model with the approaches of the USA, Israel, and Poland. Their experience shows that it is possible to build an effective regulatory and institutional framework that integrates operational response, strategic planning, and the participation of diverse security actors. Table 3 summarises these countries' legislative measures, organisational models, and levels of effectiveness, while highlighting the implications of the identified differences for Ukraine.

Table 3. Key approaches to cyber defence in the USA, Israel, Poland, and Ukraine

Country	Legislation	Cyber defence model	Effectiveness	Meaning for Ukraine
The USA	National Cybersecurity Strategy (The White House, 2023); Cyber Incident Reporting for Critical Infrastructure Act of 2022 (Cybersecurity and Infrastructure Security Agency, 2022)	Network federalism, active opposition, private partners	High dynamism, fast response	It demonstrates the importance of engaging the private sector and municipalities and developing shared responsibility for cybersecurity. Ukraine should integrate business and the civilian sector into its defence system.
Israel	Israel National Cyber Directorate (INCD)	Proactive disruption strategy	Successful warning logic	It provides an example of the creation of a coordination centre and the transition from reactive actions to preventive threat modelling. For Ukraine, this means centralising responsibility and implementing crisis scenarios in advance.
Poland	Cybersecurity strategy of the Republic of Poland for 2019-2024 (Ministry of Digital Affairs, 2019),	Cyber Command establishment	Effective civil-military cooperation	It demonstrates the value of integrating cyber strategies into military doctrine and engaging civilian structures simultaneously. It is important for Ukraine to develop a mechanism for multilevel cooperation, especially with NATO and EU partners.
Ukraine	Cybersecurity Strategy of Ukraine (President of Ukraine, 2021), plans of the Cabinet of Ministers, orders of the SSU	Reactive model, fragmented coordination	Lack of a unified system model	Differences with the leading models indicate the need to create a unified coordination centre, specify responsibilities in legislation, integrate business and civil society, and strengthen preventive mechanisms.

Source: compiled by the authors

The United States is a leader in shaping global cybersecurity policy, offering a model based on the principles of public-private partnerships, multi-level governance, and strategic foresight. The US legislative framework is constantly updated. In 2022-2024, more than 10 new regulations on cyber incidents, supply chain security, and cyber education were adopted (Lee & Chua, 2023). The key regulatory document is the National Cybersecurity Strategy (The White House, 2023), which envisages a shift from reactive to proactive threat deterrence. It also establishes the responsibility of the private sector for the protection of critical infrastructure. The strategy is based on the concept of shared responsibility of the state, business, and citizens for digital security (Weaver, 2022). The US Congress also passed the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (Cybersecurity and Infrastructure Security Agency, 2022), which requires infrastructure operators to report incidents within 72 hours.

The Cybersecurity and Infrastructure Security Agency (CISA) is the central coordinator, which operates within the Department of Homeland Security. The CISA performs the functions of rapid response, standardisation, risk analysis, training, and technical assistance. Its strategy is based on proactive actions, active use of AI to monitor threats, and close coordination with the IT sector. Moreover, the National Security Council and the Department of Defence, and the US Cyber Command coordinate actions in case of state-level cyberattacks. Grant support programmes for cyber resilience for municipalities, states and educational institutions were introduced. A distinctive feature of the US model is the focus on cyber research by the National Institute of Standards and Technology and leading universities (Weaver, 2022).

The Israeli model is an example of a centralised integrated approach to cybersecurity in the face of the constant threat of terrorist attacks. Back in 2011, the Israel National Cyber Bureau was established, and later its functions were transferred to the Israel National Cyber Directorate (INCD), which is directly subordinated to the Prime Minister of Israel. The INCD combines operational functions with political and strategic planning, control of cyber infrastructure, development of standards, and coordination with the army, intelligence, and the private sector. A specific feature of the

Israeli system is the model of responsibility at the point of threat. It means that organisations that own digital assets are responsible for their protection but are obliged to act in accordance with the INCD standards (Hassib & Shires, 2024).

Israel carries out centralised detection and prevention of attacks, using traditional analytical tools and AI. However, prevention is a key element; the focus is not only on incidents but on potential attack scenarios modelled in real time. Moreover, legislation provides a framework for cooperation between the state and IT companies in terms of information exchange, confidentiality, and personal data protection. In addition, military education in cybersecurity (e.g., the Unit 8200) provides highly qualified personnel for further use in the civilian sector (Tabansky, 2020).

Poland strengthened its cyber infrastructure significantly in recent years. In 2019, the Cybersecurity Strategy of the Republic of Poland for 2019-2024 was approved (Ministry of Digital Affairs, 2019), prioritising cyber defence, the development of a national early warning system, and closer cooperation with allies. In this regard, the Cyberspace Defence Forces were established within the Armed Forces of Poland. They are responsible for responding to cyber incidents promptly, ensuring information resilience, and protecting military infrastructure (Kitler, 2021). Moreover, the Government Centre for Security functions as a civilian coordinator responsible for early detection and warning. Furthermore, the annual cyber deterrence exercises involving NATO, business, and academic institutions are conducted. In addition, Poland implemented the EU NIS2 Directive (European Parliament and of the Council, 2022) and adopted a number of acts on critical infrastructure, e-government cyber defence, cyber hygiene, and cyber education. These initiatives are implemented in parallel with the increased involvement of the private sector in creating solutions by the Polish Institute for Cybersecurity and support for innovative start-ups (Sulowski, 2023).

As compared with these models, Ukraine looks vulnerable. Despite being in a state of full-scale war, it still does not have a unified coordination body in cybersecurity. Moreover, its legislative framework remains fragmented, while strategic documents are mostly declarative. Although the

Cybersecurity Strategy of Ukraine was approved in 2021 (President of Ukraine, 2021), it is limited by the lack of a coordination centre, imperfect mechanisms of interaction between authorities, and weak institutional structure. The regulatory framework lacks a separate law on cyber defence and legal mechanisms for involving civil initiatives in the cyber defence system. The existence of incident response centres (CERT-UA) does not compensate for the actual distrust between agencies and excessive centralisation with a lack of resource autonomy (Shypilova, 2019). Therefore, in 2022-2023, cases of duplication of functions, delays in decision-making, and lack of transparent communication were recorded (Kravchuk et al., 2024).

The large-scale cyberattacks of 2022-2023 exposed serious structural deficiencies in the response and coordination system between key institutions, i.e., the SSU, the SSSCIP, and the Cabinet of Ministers of Ukraine. The Ukrainian cyber defence model is designed to disperse responsibility between different structures, which reduces the effectiveness of decision-making and slows down the response time to threats (Abibok, 2022). Despite the integrated model of risk management and coordination declared in the 2021 Strategy, the interaction remained fragmented. This is confirmed by independent analytical reports and specific crisis incidents. Thus, in January 2022, a cyberattack took down more than 70 government websites, such as the Cabinet of Ministers of Ukraine website and the Diia portal. In 2022, CERT-UA also recorded more than 2,000 incidents. However, a significant number of them were handled only after the fact, without signs of preventive deterrence (State Service of Special Communications and Information Protection of Ukraine, 2024b). This indicates the absence of an effective crisis protocol and a single cyber incident management centre in the context of hybrid warfare (CERT-UA, 2022; Scroxton, 2023).

Nevertheless, the Ukrainian experience has unique features. Ukraine is the first country to implement large-scale digitalisation of public services during active warfare (Holovkin et al., 2023). Second, Ukrainian society demonstrates a high level of digital competence, readiness for self-defence, and mobilisation of volunteer cyber initiatives (Nizovtsev et al., 2022). These factors should be integrated into a formalised cyber

deterrence system. However, without a clear regulatory framework and organisation, Ukraine risks remaining vulnerable to multi-pronged hybrid threats. Durin the post-war recovery, such threats could have critical consequences for the sustainability of public administration.

The comparison reveals distinct approaches to cybersecurity management. Thus, the USA emphasises a decentralised system with strong private sector involvement; Israel prioritises centralised preventive threat management; Ukraine remains fragmented and reactive; while Poland achieves a balance between military and civilian structures, enabling multi-level coordination. For Ukraine, the Polish experience is especially relevant for improving cooperation between the Ministry of Defence, the SSU, the SSSCIP, and civilian institutions. At the same time, Ukraine must move beyond excessive state-centricity by creating conditions for IT business participation and empowering local governments.

International experience offers several adaptable solutions. The US model suggests establishing a single coordinating body with real-time analytical and response capacities. The Israeli model underscores the value of formalised partnerships with IT volunteers and civil cyber initiatives. The Polish model demonstrates the effectiveness of regional CERT centres, which could be replicated through a network of regional cyber resilience centres within Ukraine's administrations. Overall, Ukraine needs to synthesise these three elements: public-private integration from the USA, centralised prevention from Israel, and military-civilian cooperation from Poland. Such a model would provide a comprehensive framework for cyber deterrence, tailored to the conditions of martial law and the demands of post-war recovery.

Empirical data confirms the need for a profound transformation of the public administration system, considering constant cyber threats as a factor of political influence. Therefore, digital infrastructure should be viewed as a strategic resource of public authority, the vulnerability of which directly affects the legitimacy and effectiveness of the state in conditions of war and post-war recovery. The study results confirm the need to rethink Ukraine's cyber strategy as an integrated component of public policy. In the context of hybrid warfare, cyberspace ceases to be merely a vulnerable

environment and becomes an impetus for political transformation, requiring appropriate institutional, legal and strategic changes. Ukraine has the potential to implement the best practices of Israel and Poland, but to do so, it must overcome fragmentation in governance and formalism in responding to threats.

Having analysed cases from Ukraine, Poland, Israel, and the United States, it is possible to classify the political effects of cyberattacks on public administration. Destabilisation effects include short-term disruptions in the work of government bodies, which undermine the state's ability to respond quickly to crises. Fragmentation effects refer to consequences that erode administrative unity and weaken the synchronisation of actions by key public authorities. A striking example is the large-scale attack on financial infrastructure in February 2023, i.e., despite the clearly coordinated nature of the attack, interagency coordination began only 48 hours later. Transformation effects are manifested in long-term changes in institutional practices, the regulatory framework and strategic approaches in the field of public administration. Such consequences can be positive (strengthening cyber infrastructure, creating new institutions) and negative (excessive centralisation, restricting citizens' rights under the pretext of strengthening security). Delegitimisation effects are linked to the undermining of trust in government structures and digital interaction tools. A telling example was the mass complaints about the performance of the Diia portal after the cyberattack in November 2022. Inertia effects are manifested in delayed decision-making or in the reproduction of outdated and ineffective cyber defence models.

3.4. A hypothetical model of interaction between cyberspace and political processes

Empirical observations help to identify four key trends that are important for modelling. First, there is an escalation in the number of incidents and an increase in the density of events in state SOCs. This reflects an increase in the intensity of threats and improvements in the ability to detect them (State Service of Special Communications and Information Protection of Ukraine, 2024b; State Cyber Protection Centre State Special Communi-

cations, 2024). Secondly, there is a noticeable event- and season-related wave-like pattern to the attacks. Their peaks coincide with significant military and political events (in particular, energy strikes), which indicates a convergence of cyber activity with kinetic operations (Greenberg, 2023). Thirdly, the dominant tactics are changing: instead of high-profile destructive actions, the emphasis is shifting to persistent reconnaissance, phishing, and compromise of communication chains, while DDoS attacks have become merely a tool of information pressure (Cert-EU, 2023; Cyber Incident Response Operations Centre, 2024). Fourthly, a two-domain vulnerability space is forming. It means that attacks are directed at central registries and portals, and at regional or local nodes that ensure the continuity of administrative and life-support services (Canadian Centre for Cyber Security, 2022).

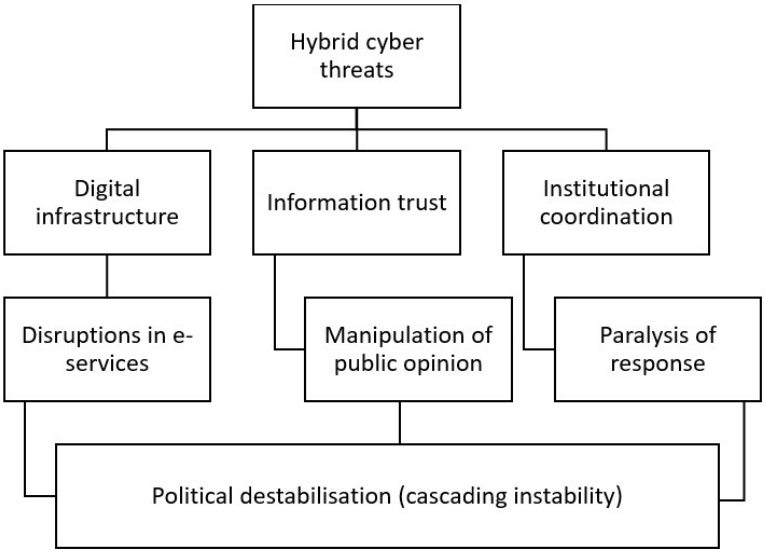
For visualization purposes, it is advisable to build time series based on monthly or weekly intervals of CERT-UA/SSSCIP incident publications, while overlaying event markers such as missile strikes, announcements of mobilization or reform decisions, and visible service failures. The cartographic heat map should reflect the concentration of incidents or attempted attacks in the following areas: central government domains and registries, regional state administrations and city councils, and energy and telecommunications facilities, highlighting corridors of increased risk in the East and South of Ukraine. The combination of temporal and spatial data confirms the provisions of the hypothetical model of cyber convergence of management vulnerabilities. In other words, the synchronisation of attacks in the technical, informational, and institutional dimensions increases the likelihood of cascading instability in public administration (Cert-EU, 2023).

The CERT-UA/SSSCIP open data is partially aggregated and does not always contain complete geographical attribution of incidents. Therefore, the spatial analysis reflects a conservative assessment of risk concentration and requires validation on extended telemetry samples, such as SOC data or ICS event logs, in further research. Moreover, not all recorded attacks were publicly confirmed by state authorities, which is partly explained by political expediency. The geospatial distribution of attacks poses another

threat. According to the heat map, regional digital services in the Kharkiv, Dnipropetrovsk, Odesa, Zaporizhzhia, and Mykolaiv regions are also vulnerable. This is explained by the technical limitations of local infrastructure and the growing role of regional military administrations in implementing state policy in wartime.

In hybrid warfare, cyberspace appears as a technical tool for ensuring the functioning of state services and a multidimensional environment that influences political processes (Kortukova et al., 2023). In other words, political processes are integrated into cyberspace and depend on its stability. For example, technical failures turn into administrative delays, distorted information reduces trust in official communications, and coordination failures between agencies complicate the development of consolidated decisions (Rabinovych et al., 2025). This gives rise to the phenomenon of cascading instability, when the simultaneous action of several types of threats creates the effect of political shock. As a result, public administration faces a double challenge, i.e., the need to restore digital services and restore public confidence in the effectiveness of the authorities. The suggested hypothetical cyber convergence of management vulnerabilities model illustrates this interconnection (Figure 1).

Figure 1. Cyber convergence of management vulnerabilities model



Cyberattacks on digital infrastructure lead to disruptions in the provision of public services, which creates fertile ground for manipulating public opinion. In turn, the loss of trust in information causes imbalances in interagency coordination and paralysis in responding to crisis situations. The combination of these factors creates political destabilisation, which can affect the internal legitimacy of the government and the international image of the state. This model demonstrates how attacks in cyberspace affect the functioning of the state apparatus, public trust and the decision-making process simultaneously, creating cascading instability.

Thus, the interaction between cyberspace and political processes during wartime should be viewed as a single dynamic system. Its key characteristic is the interdependence of technical and political vulnerabilities, which reinforce each other. Understanding this interaction facilitates creating new approaches to public administration, where cyber defence is seen as a political function that determines the stability and resilience of the state in hybrid warfare.

3.5. Management reforms in wartime: key areas

The Russian full-scale aggression against Ukraine has highlighted the need for situational measures to respond to hybrid threats and systemic reforms of public administration. The pre-reform public administration was designed for peacetime and thus faced the challenge of adapting to anti-crisis regimes. This was facilitated by the introduction of martial law, the expansion of the powers of the President of Ukraine, the National Security and Defence Council of Ukraine, and military administrations, which were given special functions and status (Nehara et al., 2025). In legal terms, this was accompanied by the introduction of military procedures, such as accelerated procurement, simplified budgeting, and temporary restrictions, which are assessed in terms of necessity and proportionality.

At the same time, even during the war, reforms continued, particularly decentralisation. Despite martial law, support for local self-government reform grew. Thus, 63% of respondents approved of it in 2021, compared to 77% during martial law (Centre of Expertise for Multilevel Governance, 2022). Decentralisation ensured local capacity and adaptability (Oliychenko et al., 2024). Moreover, digital transformation became a key component of crisis management through the introduction of electronic government services, digital registries and platforms

proved key to maintaining the continuity of public services, logistics chains and communications (Gustafsson et al., 2025). In the defence procurement sector, a new state logistics operator (DOT) emerged with a transparent DOT-Chain platform, which reduced costs by 25% and ensured that 95% of contracts for requested goods are fulfilled in accordance with NATO standards (Kullab, 2024).

Furthermore, anti-corruption reform remained a priority (Hudz, 2024). The Verkhovna Rada of Ukraine abandoned attempts to subordinate the main anti-corruption bodies (NABU, SAP) to the Prosecutor General thanks to active civic response (Halushka, 2025). In the judiciary, Ukraine continued to implement reforms, including the creation of high specialised courts to resolve political disputes in order to fulfil the IMF's conditions for continuing financing in the amount of $15,6 billion (Peleschuk & Lewis, 2025). Overall, the judicial reform included the creation of the High Council of Justice, the High Qualification Commission of Judges, the Public Integrity Council, and the Anti-Corruption Court.

Civil society continues to support reform implementation strategies even during wartime. As Chatham House notes, war can be a period for establishing institutions that will gain the trust of donors and society (Lutsevych, 2024). Transparency International Ukraine (2024) highlights key areas such as an anti-corruption environment, effective reconstruction, reform of the Accounting Chamber and the State Audit Service, which are critical for the military and post-war stability. European analysts emphasise that the war destroyed previous reform blocks. As a result, Ukraine must take advantage of this opportunity by preserving pluralism, by not concentrating excessive power in the hands of the Presidential Administration or security forces, and continuing judicial reform and the fight against oligarchs (Wilson, 2023).

Moreover, institutional reform took place in the area of cybersecurity coordination: the powers of the SSSCIP was expanded and new mechanisms for interaction between the Ministry of Digital Transformation of Ukraine, the SSU and sectoral management bodies were created (Ponomarov et al., 2023). This helped to shift from a fragmented response to more centralised risk management models and had a positive impact on the speed of response during large-scale attacks. However, excessive centralisation continues to pose risks of reduced flexibility and delays in decision-making at the regional level. Furthermore, the war stimulated the integration of the private sector and the IT community into the state

cyber defence system. While such cooperation was mostly informal until 2022, it gradually became institutionalised during martial law. For instance, platforms for sharing information about incidents were created, and stable networks of interaction between state bodies and technology companies were formed.

In addition, there is ongoing digitalisation of management under martial law. Owing to the Diia portal and other digital services, government services remained accessible during massive attacks. This proves a transition from paper bureaucracy to a digital administrative model being more resilient in during the crisis. A reform of strategic planning in security was also initiated, which considers cyber threats a key element of national security alongside military and economic components. Finally, the war provoked decentralisation in cyber defence, as there was a need to transfer some powers and resources to the regions. The establishment of local incident response teams and the development of regional resilience centres created the conditions for a more flexible management model in the future.

Despite the progress made, there are still structural problems that need to be addressed. Particular attention should be paid to the fragmentation of the regulatory framework, a significant part of which is of Soviet origin and does not correspond to new hybrid threats. Although the Cybersecurity Strategy of Ukraine (President of Ukraine, 2021) was adopted, Ukraine's regulatory framework remains fragmented and only partially harmonised with European standards (NIS2, GDPR). The absence of a specialised law on cyber defence and clear procedures for interaction between authorities limits the effectiveness of strategic planning and reduces the state's ability to counter multi-level hybrid threats. The shortage of highly qualified personnel in cybersecurity in the public sector remains the key challenge. During the war, this problem is partially resolved by the mobilisation of IT volunteers and the development of public cyber initiatives. Excessive centralisation of cyber defence management limits the ability of regions to respond to attacks quickly, while the low level of digital literacy among officials creates a favourable environment for successful attacks using social engineering.

The SSSCIP, CERT-UA, the Ministry of Digital Transformation of Ukraine, and sectoral CERT structures demonstrated their ability to shift from preventive to crisis management of cyber incidents. Despite massive attacks (up to 15-20 major incidents per day during peak periods), it was possible to avoid a systemic collapse of the digital infrastructure. This demonstrates a high level of operation-

al coordination. Despite the intensity of the attacks, key digital services (Diia, Prozorro, tax services) continued to function. The use of cloud technologies, server geospatial distribution, and international support (Microsoft, Amazon Web Services, Google) helped to maintain the availability of administrative services even during massive missile and cyberattacks. This increased citizens' trust in the state in conditions of uncertainty.

In the post-war period, when the reconstruction of the state will be accompanied by increased geopolitical risks and internal political transformations, the role of cyberspace will grow. Therefore, it is important to shape digital sovereignty, considering the best practices of allies and the specifics of the Ukrainian context. In this regard, it is worth offering a number of recommendations that could increase the effectiveness of the cybersecurity strategy and restore administrative capacity. Thus, it is necessary to update the regulatory framework, bringing it into line with NATO and EU standards and removing archaic provisions.

Furthermore, it is essential to invest in human resource development by creating specialised educational programmes for the public sector and raise cyber awareness of civil servants. It is also advisable to expand decentralisation in cyber defence by creating regional cyber resilience centres with resource and organisational autonomy. In addition, integration with international response systems should be intensified by expanding participation in joint exercises. Finally, a key focus should be on engaging the private sector and institutionalising cooperation with the IT community, which will increase the flexibility and technological effectiveness of the national cyber defence system. In summary, the results of the study indicate the need to transform Ukraine's cyber strategy from a predominantly technocratic tool into a full-fledged component of national security policy and modernisation of management practices. In summary, the study results indicate the need to transform Ukraine's cyber strategy from a predominantly technocratic tool into a full-fledged component of national security.

4. Conclusions

The study identified key features of the transformation of public administration in Ukraine in hybrid warfare and under massive cyber threats. The analysis showed that contemporary challenges in the digital sphere went beyond technical incidents and affected institutional stability, public trust, and the state's ability

to implement management decisions. Moreover, a typology of the latest hybrid threats was suggested, covering the infrastructural, informational-psychological and institutional-network dimensions, which created a political shock effect and could paralyse the functioning of the state apparatus.

The developed model of interaction between cyberspace and political processes showed that cyberattacks had a cascading nature. In other words, local technical incidents could escalate into a crisis of confidence and cause managerial destabilisation. This was confirmed by empirical data on the temporal dynamics of attacks and the spatial concentration of hot spots in the public sector. Observations revealed patterns of peak waves of attacks associated with critical phases of war and the vulnerability of key digital platforms.

The assessment of the effectiveness of Ukraine's cybersecurity strategy demonstrated its ability to ensure the continuity of key government functions during periods of large-scale attacks. At the same time, the strategy had a number of structural problems: fragmentation of the regulatory framework, staff shortages, excessive centralisation and insufficient digital literacy among civil servants. These factors limited the potential of the cyber defence system to restore full administrative capacity.

The practical significance of the results lies in the formulation of recommendations for improving the cyber resilience of public authorities. These include modernising the legislative framework, developing professional human resources, creating regional cyber resilience centres, institutionalising cooperation with the IT community, and integrating it into international security networks. The implementation of these measures can enhance the security and ensure the stability of public administration during wartime and the post-war period.

Despite the warfare, the ongoing reforms lay the foundation for the modernisation of the public administration in the post-war period. The institutional consolidation in cybersecurity, partnerships with the private sector and the IT community, accelerated digitisation of services, development of strategic planning, and decentralisation of security functions are shaping a new management model that will be more flexible, transparent, and sustainable. These developments will make it possible to combine reconstruction tasks with the modernisation of public administration. They in turn will ensure Ukraine's integration into the European space as a state capable of countering hybrid threats effectively.

Nevertheless, the study has several limitations. Firstly, the analysis mainly covers short- and medium-term effects, while long-term consequences remain uncertain, particularly regarding the risk of institutionalising excessive centralisation after the war and a possible imbalance between the branches of government. Secondly, the lack of empirical data limits the quantitative assessment of the effectiveness of reforms, as the available observations are mainly descriptive and normative. Thirdly, the study focuses on the national level, leaving out local specifics and the impact of reforms on communities that bear a significant burden in providing basic services.

Therefore, the results should be considered an interim analysis that requires further research of positive effects and potential risks of military reforms. In this regard, further research should focus on studying the long-term political consequences of hybrid cyber threats, developing models of interagency coordination in crisis situations, and comparing the experiences of countries that have been in a state of hybrid confrontation. Finally, it is important to study the cyber strategy integration into the broader national security system as a tool for protecting digital sovereignty and strengthening state capacity in the 21st century.

References

Abibok, Yu. (2022). Cyberattacks undermine Ukraine's security. *Institute for War & Peace Reporting*. Retrieved from https://iwpr.net/global-voices/cyberattacks-undermine-ukraines-security

Bondarenko, S., Niziaieva, V., Kravchenko, M., Kaliuha, Ye., Kolisnichenko, R., & Tsumariev, M. (2025). Modernization of Administrative Control over the Legality of Decisions of Local Self-Government Bodies of Ukraine. *Evropský Politický a Právní Diskurz, 12*(1), 31-44. https://doi.org/10.46340/eppd.2025.12.1.4

Canadian Centre for Cyber Security. (2022). Cyber threat bulletin: Cyber threat activity related to the Russian invasion of Ukraine. Retrieved from https://www.cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf?utm_source

Centre of Expertise for Multilevel Governance. (2022). Ukraine: in wartime support to decentralisation reform increased. Retrieved from https://www.coe.int/en/web/centre-of-expertise-for-multilevel-governance/-/ukraine-in-wartime-support-to-decentralisation-reform-increased?utm_source

Cert-EU. (2023). Russia's war on Ukraine: one year of cyber operations 24 February 2022 – 24 February 2023. Retrieved from https://cert.europa.eu/static/MEMO/2023/TLP-CLEAR-CERT-EU-1YUA-CyberOps.pdf?utm_source

CERT-UA. (2022). First annual report on the results of the vulnerability detection system and response to cyber incidents and cyberattacks. Retrieved from https://cert.gov.ua/article/17696

Cherep, O., Kaliuzhna, Y., Mykhailichenko, L., Markova, S., & Naumenko, Y. (2025). Formation of a strategy for countering and identifying AI technologies in the fight against disinformation under martial law. *Technology Audit and Production Reserves*, *2*(2(82), 74-79. https://doi.org/10.15587/2706-5448.2025.327157

Cyber Incident Response Operations Centre. (2024). 2024 Annual report: Vulnerability detection and cyber incident / cyberattack response system. Retrieved from https://scpc.gov.ua/api/files/4560c0ba-c6c0-4935-b48d-0232dd659df3?utm_source

Cybersecurity and Infrastructure Security Agency. (2022). Cyber Incident Reporting for Critical Infrastructure Act of 2022. Retrieved from https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

European Parliament and of the Council. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Retrieved from http://data.europa.eu/eli/dir/2022/2555/oj

Greenberg, A. (2023). Sandworm hackers caused another blackout in Ukraine - During a missile strike. *Wired.* Retrieved from https://www.wired.com/story/sandworm-ukraine-third-blackout-cyberattack/?utm_source

Gustafsson, M., Matveieva, O., Wihlborg, E., Borodin, Y., Mamatova, T., & Kvitka, S. (2025). Adaptive governance amidst the war: Overcoming challenges and strengthening collaborative digital service provision in Ukraine. *Government Information Quarterly, 42*(3), article number 102056. https://doi.org/10.1016/j.giq.2025.102056

Halushka, O. (2025). Ukraine's anti-corruption reforms are more vital than ever during wartime. *Atlantic Council.* Retrieved from https://www.atlanticcouncil.org/blogs/ukrainealert/ukraines-anti-corruption-reforms-are-more-vital-than-ever-during-wartime/?utm_source

Hassib, B., & Shires, J. (2024). Digital recognition: cybersecurity and internet infrastructure in UAE–Israel diplomacy. *International Affairs, 100*(6), 2399-2418. https://doi.org/10.1093/ia/iiae233

Holovkin, B., Cherniavskyi, S., & Tavolzhanskyi, O. (2023). Factors of cybercrime in Ukraine. *Relacoes Internacionais no Mundo Atual, 3*(41), 464-488.

Hudz, V. (2024). Expert conclusion as a key source of evidence in cases of corruption offenses by officials. *Legal Horizons, 22*(3), 34-45. https://doi.org/10.54477/LH.25192353.2024.3.pp.34-45

Kitler, W. (2021). The Cybersecurity Strategy of the Republic of Poland. In Chałubińska-Jentkiewicz, K., Radoniewicz, F., & Zieliński, T. (Eds.), *Cybersecurity in Poland* (pp. 137–153). Cham: Springer. https://doi.org/10.1007/978-3-030-78551-2_9

Kortukova, T., Kolosovskyi, Y., Korolchuk, O.L., Shchokin, R., & Volkov, A.S. (2023). Peculiarities of the legal regulation of temporary protection in the European Union in the context of the aggressive war of the Russian Federation against Ukraine. *International Journal for the Semiotics of Law, 36*(2), 667-678. https://doi.org/10.1007/s11196-022-09945-y

Kravchuk, M., Kravchuk, V., Hrubinko, A., Podkovenko, T., & Ukhach, V. (2024). Cyber security in Ukraine: Theoretical view and legal regulation. *Law, Policy and Security, 2*(2), 28-38. https://doi.org/10.62566/lps/2.2024.28

Kullab, S. (2024). Ukraine's reformed military procurement agency drives the country's NATO ambitions. The Associated Press. Retrieved from https://apnews.com/article/russia-ukraine-war-nato-reforms-military-procurement-f0483561c9d402697d7a67dd43ae844d

Lee, C.S., & Chua, Y.T. (2023). The role of cybersecurity knowledge and awareness in cybersecurity intention and behaviour in the United States. *Crime & Delinquency, 70*(9), 2250-2277. https://doi.org/10.1177/00111287231180093

Legenkyi, M., Piankivska, L., & Tolbatov, A. (2025). Legal basis for cybersecurity in Ukraine under martial law. *Ceur Workshop Proceedings, 3925*, 334-342.

Lutsevych, O. (2024). *Ukraine's wartime recovery and the role of civil society. Chatham House survey of Ukrainian CSOs – 2024 update.* London: Chatham House. Retrieved from https://www.chathamhouse.org/sites/default/files/2024-06/2024-06-05-ukraine-wartime-recovery-role-civil-society-lutsevych.pdf.pdf?utm_source

Ministry of Digital Affairs. (2019). Cybersecurity strategy of the Republic of Poland for 2019-2024. Retrieved from https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/PL_NCSS_2019_en.pdf

Ministry of National Defence of the Republic of Poland. (2022). Analysis of the cyberattack on Ukrainian government resources. *CSIRT of the Ministry of National Defence.* Retrieved from https://csirt-mon.wp.mil.pl/aktualnosci/analysis-of-the-cyber-attack-on-ukrainian-government-resources/?utm_source

National Cybersecurity Coordination Centre. (2023). Review of cybersecurity news in Ukraine, tendencies, and world events related to the First World Cyber war. Retrieved from https://www.rnbo.gov.ua/files/%D0%9D%D0%9A%D0%A6%D0%9A/2023/Cyber%20digest_August_2023_EN.pdf?utm_source

National Cybersecurity Coordination Centre. (2024). Cybersecurity Threat Landscape of Ukraine in 2023. Retrieved from https://understandingcyberwar.org/wp-content/uploads/2024/09/Proekt_3_en.pdf?utm_source

Nehara, R., Kalchuk, O., Riabchenko, O., Kapitanets, S., & Marusiak, O. (2025). System of public administration entities in times of war: the Ukrainian experience. *CERIDAP, 2*, 170-190. https://doi.org/10.13130/2723-9195/2025-2-20

Nizovtsev, Y.Y., Lyseiuk, A.M., & Kelman, M. (2022). From self-affirmation to national security threat: Analyzing Ukraine's foreign experience in countering cyberattacks. *Revista Cientifica General Jose Maria Cordova, 20*(38), 355-370.

Okunovska, Yu., & Prymush, M. (2024). Local self-government in Ukraine in the context of a full-scale invasion. *Evropský Politický a Právní Diskurz, 11*(3), 43-50. https://doi.org/10.46340/eppd.2024.11.3.4

Oliychenko, I., Ditkovska, M., & Klochko, A. (2024). Digital transformation of public authorities in wartime: The case of Ukraine. *Journal of Information Policy, 14*, 686-746. https://doi.org/10.5325/jinfopoli.14.2024.0020

Peleschuk, D., & Lewis, B. (2025). Ukraine to set up high-level courts as part of reform drive. *Reuters*. Retrieved from https://www.reuters.com/world/europe/ukraine-set-up-high-level-courts-part-reform-drive-2025-02-26/?utm_source

Polityuk, P. (2022). Massive cyberattack hits Ukrainian government websites as West warns on Russia conflict. *Reuters*. Retrieved from https://www.reuters.com/technology/massive-cyberattack-hits-ukrainian-government-websites-amid-russia-tensions-2022-01-14/?utm_source

Ponomarov, O.A., Pyvovarchuk, S.A., Kozubtsova, L.M., Kozubtsov, I.M., Bondarenko, T.V., & Tereshchenko, T.P. (2023). Hybrid construction of cyber security system: Administrative and legal principles of military-civil cooperation. *Cybersecurity: Education, Science, Technique, 3*(19), 109-21. https://doi.org/10.28925/2663-4023.2023.19.109121

President of Ukraine. (2021). Decree No. 447/2021 on the decision of the National Security and Defence Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine". Retrieved from https://zakon.rada.gov.ua/laws/show/447/2021#n12

Rabinovych, M., Brik, T., Darkovich, A., Hatsko, V., & Savisko, M. (2025). Ukrainian decentralization under martial law: challenges for regional and local self-governance. *Post-Soviet Affairs*, 1-25. https://doi.org/10.1080/1060586X.2025.2520167

Scroxton, A. (2023). Ukraine cyber teams responded to more than 2,000 attacks in 2022. *Computer Weekly*. Retrieved from https://www.computerweekly.com/news/252529292/Ukraine-cyber-teams-responded-to-more-than-2000-attacks-in-2022

Shypilova, Yu. (2019). *Legal framework for Ukrainian cybersecurity: overview and analysis*. Arlington: International Foundation for Electoral Systems.

Simons, G., Danyk, Y., & Maliarchuk, T. (2020). Hybrid war and cyber-attacks: creating legal and operational dilemmas. *Global Change, Peace & Security*, *32*(3), 337-342. https://doi.org/10.1080/14781158.2020.1732899

State Cyber Protection Centre State Special Communications. (2024). Q4 2023 Report. Retrieved from https://scpc.gov.ua/en/articles/341?utm_source=

State Service of Special Communications and Information Protection of Ukraine. (2024b). The CERT-UA Team has processed 2,543 cyber incidents over 2023. Retrieved from https://cip.gov.ua/en/news/uryadova-komanda-cert-ua-v-2023-roci-opracyuvala-2543-kiberincidenti?utm_source=

State Service of Special Communications and Information Protection of Ukraine. (2024a). Russian cyber operations: Analysis for the second half of 2023. Retrieved

from https://cip.gov.ua/services/cm/api/attachment/download?id=68775

Stokel-Walker, C. (2022). Ukraine's cyberwar chief sounds like he's winning. *Wired.* Retrieved from https://www.wired.com/story/yurii-shchyhol-urkaine-cyberwar-russia/?utm_source

Sulowski, S. (2023). *Security challenges at the dawn of a new international order.* Berlin: Peter Lang Verlag.

Tabansky, L. (2020). Israel Defence Forces and national cyber defence. *Connections: The Quarterly Journal, 19*(1), 45-62. https://doi.org/10.11610/Connections.19.1.05

The White House. (2023). National Cybersecurity Strategy. Retrieved from https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Transparency International Ukraine. (2024). Wartime and post-war resilience: Reform fundamentals in Ukraine. Retrieved from https://ti-ukraine.org/en/news/wartime-and-post-war-resilience-reform-fundamentals-in-ukraine/?utm_source

Voloshchuk, Y., Lavruk, N., Derlytsia, A., Havryliuk, V., & Kulii-Demianiuk, Y. (2025). The role of public investment in innovative projects during martial law. *Economics of Development, 24*(1), 45-46. https://doi.org/10.63341/econ/1.2025.45

Weaver, J.M. (2022). *The U.S. cybersecurity and intelligence analysis challenges.* London: Palgrave Macmillan Cham.

Wilson, A. (2023). Reformation nation: Wartime politics in Ukraine. *European Council on Foreign Relations.* Retrieved from https://ecfr.eu/publication/reformation-nation-wartime-politics-in-ukraine/?utm_source#summary

Yagunov, D., Polovyi, M., Melnychuk, T., Starenkyi, S., Sokalska, O., Chernousov, A., Trokhymchuk, V., & Anishchenko, V. (2023). The phenomenon of informal prison hierarchies and the simulacrum of prison subculture in contemporary power relations. *Evropský Politický a Právní Diskurz, 10*(4), 5-51. https://doi.org/10.46340/eppd.2023.10.4

Yakymchuk, O. (2019). State management of cyber security in hybrid war conditions. *Pressing Problems of Public Administration, 1*(55), 35-40. https://doi.org/10.34213/ap.19.01.04

Zvezdova, O., & Vakalyuk, A. (2022). Cyber security strategy in hybrid war. *Acta De Historia & Politica: Saeculum XXI, 03*, 82-90. https://doi.org/10.26693/ahpsxxi2021-2022.03.082