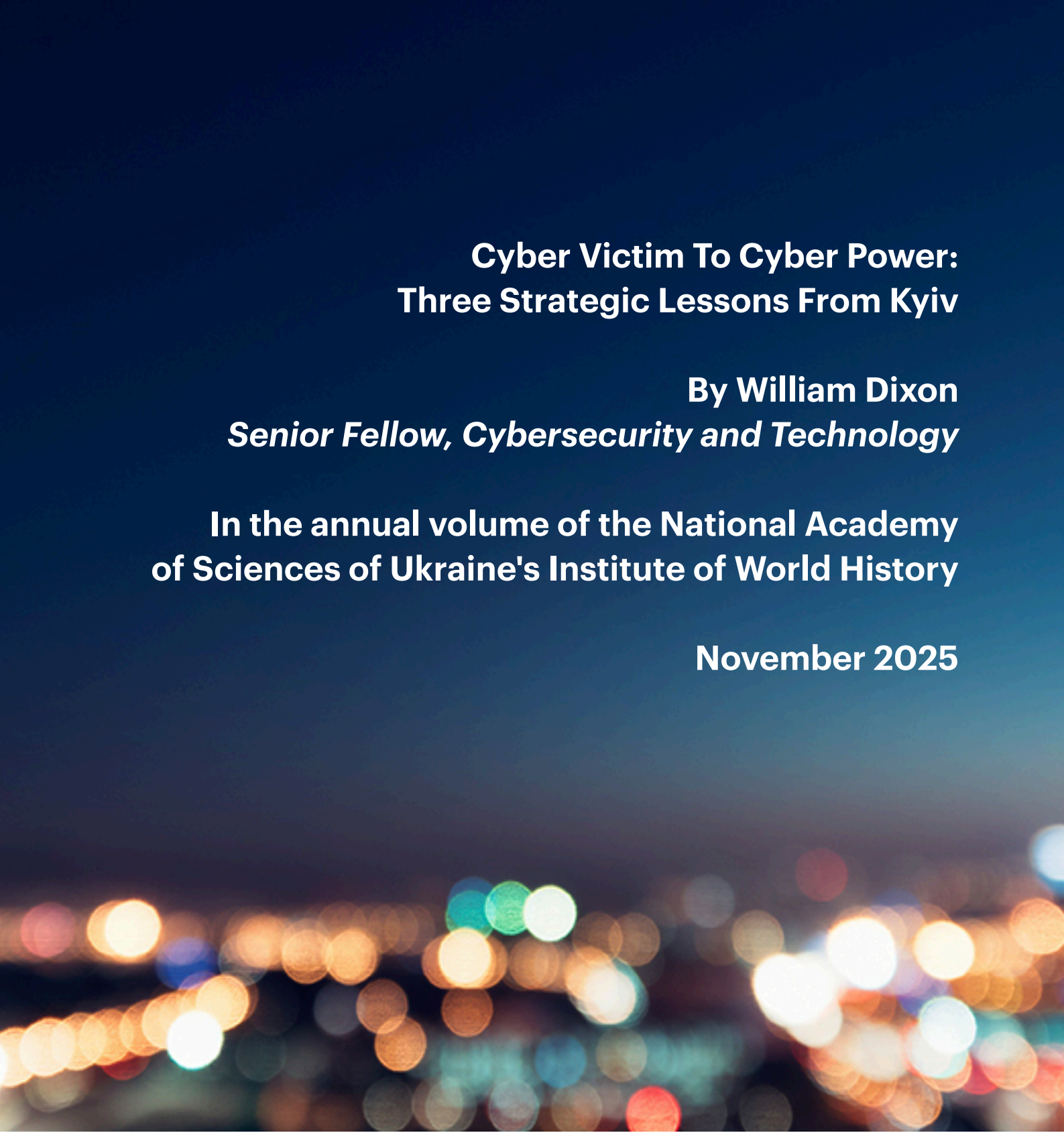
Cyber Victim To Cyber Power: Three Strategic Lessons From Kyiv

By William Dixon
Senior Fellow, Cybersecurity and Technology

In the annual volume of the National Academy of Sciences of Ukraine's Institute of World History

November 2025



UKRAINE FOUNDATION REVIEW

Ukraine Foundation

УДК 004.056 : 355.48(477)

Dixon W.

CYBER VICTIM TO CYBER POWER: THREE STRATEGIC LESSONS FROM KYIV

Ukraine's transformation from cyber victim to cyber power offers insights from the world's first sustained state-on-state cyber conflict. This article argues that institutional agility and organizational design, rather than technical superiority, determine cyber effectiveness. Drawing on open-source intelligence and comparative analysis, it distills Ukraine's experience into three strategic lessons that demonstrate how democracies can adapt under existential threat. These findings situate Ukraine's innovations within broader debates on military adaptation, democratic resilience, and hybrid conflict, offering both theoretical contributions and practical guidance for allied defense institutions.

***Keywords**: Cyber warfare, Ukraine conflict, institutional design, information operations, democratic defense, NATO strategy, cyber-physical integration*

Діксон В. Від жертви кібератак до спроможної кібердержави: три стратегічні уроки з Києва.

Перетворення України з жертви кібернетичних нападів на спроможну кібердержаву відображає перебіг першого в світі тривалого міждержавного кіберконфлікту. У цій статті стверджується, що кібернетична ефективність визначається не технічними перевагами, а інституційною гнучкістю та організаційною структурою. На основі відкритих джерел інформації та порівняльного аналізу досвід України узагальнено у три стратегічні уроки, які демонструють, як демократії можуть адаптуватися в умовах загрози їхньому існуванню. Ці висновки дають основу для розгляду інновацій України в ширшому контексті дебатів про військову адаптацію, демократичну стійкість та гібридні конфлікти, пропонуючи як теоретичний внесок, так і практичні рекомендації для оборонних інституцій союзників.

***Ключові слова**: кібервійна, конфлікт в Україні, інституційний дизайн, інформаційні операції, захист демократичної держави, стратегія НАТО, кіберфізична інтеграція.*

I. Introduction: From Cyber Victim to Cyber Power

The war in Ukraine represents the first protracted kinetic conflict between states where cyber operations have been continuously integrated across all phases of warfare. Unlike the brief cyber campaigns in Estonia (2007) or Georgia (2008), which largely involved short-lived DDoS and defacement attacks [1; 2], this conflict provides three years of sustained cyber–physical integration data. Since

Russia's February 2022 invasion, Ukraine has transformed from primarily a victim of cyber operations into an active shaper of the cyber domain—a shift that challenges conventional assumptions about the sources of cyber power [3; 4]. This transformation provides unprecedented empirical evidence for a fundamental question in security studies: what determines effectiveness in cyber conflict?

Existing literature offers competing explanations. Technological determinists emphasize advanced capabilities and sophisticated attack tools [5; 6]. Strategic theorists focus on doctrine and escalation dynamics [7; 8]. Ukraine's experience suggests a third explanation: institutional design and organizational agility matter more than technical superiority or doctrine.

This study asks: What lessons can Ukraine's cyber transformation offer for democratic states confronting authoritarian adversaries in hybrid conflict? While Thomas Rid's foundational framework of cyber operations—espionage, sabotage, and subversion—provides essential analytical categories, Ukraine's experience suggests that effectiveness across these domains depends on underlying institutional factors rather than domain-specific capabilities [9].

The central argument is that Ukraine's success stems not from technological advantages or superior operational techniques, but from institutional innovations that enabled cross-domain integration: horizontal coordination among diverse domestic and overseas actors, tactical embedding of cyber capabilities, and coherent narrative responses that span traditional operational boundaries. Jeremy Fleming, Director of GCHQ, provided a powerful third-party endorsement of Ukraine's approach, stating in August 2022 that it amounted to one of the most effective cyber defences in history [10].

While the insight that organizational design often outweighs technological superiority is not new [11; 12; 13; 14], Ukraine provides the first sustained empirical test of this principle in state-on-state cyber conflict. The novelty here lies not in the concept itself, but in demonstrating how it operates under real wartime conditions, with civil society, private sector, and state institutions fused into a coherent cyber ecosystem [15; 16].

Conceptualizing Ukraine’s Cyber Power

For the purposes of this analysis, cyber power encompasses both defensive and offensive dimensions across Rid's three operational domains. Defensively, cyber power manifests as resilience—the ability to limit an adversary's effectiveness through rapid detection, mitigation, and recovery from cyber operations. Offensively, it comprises the capacity to conduct successful operations across espionage (persistent intelligence collection), sabotage (disruption of systems and infrastructure), and subversion (shaping perceptions and narratives). Ukraine's evolution demonstrates that cyber power ultimately derives not from technical capabilities alone, but from the institutional capacity to integrate these defensive and offensive elements into coherent operational campaigns [17; 18].

Three strategic lessons emerge from this transformation. First, horizontally integrated institutions that combine government, private sector, and civil society capabilities consistently outperform centralized hierarchies in cyber conflict.

Second, cyber capabilities achieve greatest impact when embedded directly within conventional warfighting functions rather than treated as a separate strategic domain. Third, Western democracies face critical vulnerabilities in information warfare due to fragmented institutional responses that adversaries systematically exploit.

This article introduces a new mechanism of institutional adaptation: combat-driven integration. This concept describes how an existential threat can accelerate the fusion of cyber capabilities with state and civil structures, achieving a level of integration that has not been possible under peacetime conditions. Ukraine's experience provides the first sustained empirical test of this principle, showcasing a rapid, threat-accelerated transformation of cyber power. It thus presents a distinct model that contrasts with established paradigms of deliberate peacetime innovation, positing existential threat itself as the primary catalyst for rapid and profound institutional adaptation.

This study extends existing theory in three ways. First, it challenges the resource-dependency assumptions in cyber conflict theory by demonstrating how institutional design can offset material disadvantages. Second, it provides the first empirical test of networked governance theories in sustained cyber combat conditions. Third, it identifies a new mechanism for cyber—combat-driven integration—whereby existential threat accelerates institutional adaptation beyond peacetime reform capabilities.

These findings also contribute to three scholarly debates. In military innovation studies, they support theories emphasizing organizational design over technological capability [12; 13]. In cybersecurity research, they provide empirical evidence for claims about the importance of integration and persistence over isolated technical effects [17; 18]. In democratic resilience literature, they demonstrate how institutional agility can offset resource disadvantages in hybrid conflicts.

II. The Ukrainian Cyber Experience: Defying Predictions

Before Russia’s February 2022 invasion, many analysts anticipated that the conflict would “redefine cyber warfare,” with predictions of massive digital disruption from what was assessed to be a tier-one cyber power [19; 20]. These predictions were rooted in Russia's demonstrated cyber capacity during the initial conflict from 2014 onwards, where disruptive attacks on Ukrainian critical infrastructure and electoral processes revealed significant defensive vulnerabilities and a lack of coordinated national cyber strategy [21]. Instead, dramatic “lights-out” scenarios failed to materialize. Rather than a momentous first-strike cyber blitzkrieg, the conflict has featured adaptive integration of cyber capabilities across all three of Rid’s domains, revealing fundamental insights about cyber conflict dynamics.

Ukraine has transformed from primarily a victim of cyber operations into an active shaper of the cyber domain. This transformation is measurable across multiple dimensions.

Prior to 2022, Ukraine suffered major cyber incidents with limited response capability — the 2015 and 2016 power grid attacks left hundreds of thousands without electricity, and the NotPetya (2017) attack caused over US$10 billion in global damages that originated in Ukraine [19], plus the country lacked coordinated offensive cyber capabilities. By contrast, since February 2022, Ukraine has successfully defended against over 4,500 cyber attacks according to the State Service of Special Communications [22], while its offensive operations have breached Russian ministries, disrupted military logistics systems, and compromised over 800 Russian information resources according to the IT Army's public reporting [23; 24]. "Our actions are starting to look more and more like a Hollywood hacker movie, just without the popcorn." – A post on the IT Army of Ukraine's Telegram channel [23].

The shift from passive victim to active combatant represents a fundamental change in cyber posture. Critical and high-level cyber incidents plummeted from 1,048 in 2022 to 367 in 2023, and further to just 59 in 2024, according to CERT-UA reporting [25]. This represents an 81% reduction in critical incidents despite cyberattacks surging 123% in volume, demonstrating that institutional improvements in detection, mitigation, and coordination have dramatically enhanced defensive effectiveness [26]. The scale of the challenge remains significant, with Ukraine recording 4,315 total cyber incidents in 2024—approximately 12 major incidents daily—yet the success rate of critical attacks has declined substantially [27].

Across Rid's foundational categories, the conflict has revealed: Espionage Evolution: Traditional strategic cyber intelligence has evolved into tactical battlefield support systems, providing real-time targeting data for kinetic operations—fundamentally expanding cyber beyond strategic intelligence-gathering. Sabotage Constraints: While tactically valuable when synchronized with kinetic action, standalone cyber sabotage remains strategically limited, challenging assumptions about digital disruption as a substitute for conventional force. Subversion Asymmetries: Russia's volume-driven approach has achieved considerable strategic and tactical impact, while Ukraine's authenticity-driven counter-operations demonstrate that credibility can compete effectively against propaganda saturation when properly institutionalized [28].

While Rid's framework provides essential analytical categories for understanding cyber operations, Ukraine's experience reveals that operational effectiveness depends less on domain-specific capabilities than on cross-cutting institutional factors that enable integration across all three domains. This study does not treat espionage, sabotage, and subversion as separate. Instead, it shows how institutional design shapes effectiveness across the entire spectrum of cyber conflict, both defensive and offensive.

Ukraine's transformation demonstrates that the same organizational innovations—horizontal integration, tactical embedding, and coordinated response—determine effectiveness whether conducting intelligence operations, cyber-physical attacks, or information campaigns. This institutional lens explains why Ukraine could rapidly adapt across multiple domains while Russia, despite

superior technical capabilities, struggled with coordination and integration constraints rooted in political and bureaucratic structures.

For NATO allies and democratic defense institutions, the implications extend beyond the current conflict. Ukraine demonstrates that institutional reform—not merely technological investment—determines cyber readiness. As authoritarian adversaries refine hybrid warfare strategies, democratic states must adapt their organizational structures to compete effectively across all domains of conflict. Ukraine's experience offers both a model and a warning: adaptation is possible, but the window for learning may be finite.

Table 1.

The Russian-Ukraine Cyber Experience across Rid domains

Cyber Domain	Russia	Ukraine	Institutional Explanation
Espionage	GRU-led, centralized, often siloed; reported delays in intelligence flow to battlefield	Integrated ISR: state (HUR), volunteers, private partners; intelligence to battlefield within hours	Horizontal integration and rapid fusion of civil, state, and private inputs
Sabotage	Technically advanced (APT-level, CNI targeting pre-war, wipers); limited synchronization with kinetic ops	Precision-focused sabotage, often synchronized with drone/artillery strikes	Organizational agility enables cyber-physical integration
Subversion	Volume-driven "firehose of falsehood," industrial-scale disinfo campaigns targeting Western Alliance. Embedded into tactical offensives.	Authenticity-based narrative strategy coordinated by CCD + volunteers	Centralized coordination with decentralized execution produces credible counter-narratives

III. The Three Ukrainian Cyber Lessons

Lesson 1: Organizational Supremacy Versus Technical Wizardry

Ukraine's most underappreciated cyber advantage in both defensive and offensive operations lies not in advanced malware or sophisticated attack tools, but in its ability to orchestrate a horizontally integrated ecosystem that fuses inputs from foreign partners, private-sector providers, and civil society actors. This organizational innovation has at times outperformed Russia's more centralized and hierarchical model, despite Moscow's deeper technical resources.

This is rooted in a fundamental mismatch between the nature of modern cyber conflict and the deeply ingrained, hierarchical structure of the Russian state. Unlike conventional warfare, cyber operations thrive on decentralized initiative and rapid,

real-time adaptation. Russia's system, designed for top-down control and vertical information flow, created a bureaucratic bottleneck that proved too slow and inflexible to compete with Ukraine's agile, horizontally integrated network of state and non-state actors [29].

This organizational innovation has enabled Ukraine to achieve operational effects disproportionate to its resources, compensating for Russia's technical and numerical advantages through speed of adaptation and cross-sector coordination. While Russia maintains superiority in advanced persistent threats and zero-day capabilities, Ukraine's distributed model has demonstrated particular advantages in rapid cyber defense, crowd-sourced intelligence gathering, and coordinated narrative responses.

Military innovation studies show that organizational design often outweighs technology [11; 12]. Networked governance and collaborative advantage theories argue that distributed coordination can exceed the sum of its parts [31; 32]. Cyber studies add that offensive operations achieve value mainly when integrated with broader campaigns [18; 17].

The Horizontal Integration Advantage

Ukraine’s defensive cyber resilience, by contrast, rests on multi-stakeholder coordination across government, the military, private technology companies, and volunteer civilian groups. This horizontal integration advantage has been critical to Ukraine’s success. From Microsoft’s security telemetry to diaspora-led forensics and grassroots OSINT networks, this pluralistic architecture has enabled agility that centralized systems struggle to replicate [33; 34].

This horizontal integration advantage is critical to Ukraine's success and a core manifestation of combat-driven integration in Ukraine's defensive posture. The existential threat of the full-scale invasion forced a rapid, unprecedented coalition of state agencies, volunteer hackers, and foreign private-sector companies, all of which had previously operated in relative silos

The efficacy of Ukraine's horizontally integrated cyber defense model is not merely anecdotal; it is now empirically validated by official performance data. The State Service of Special Communications and Information Protection 2025 Annual report marked a clear increase in defensive resilience from 2021 to 2024. As shown in Table 1, the total volume of detected cyber incidents demonstrates a major escalation of Russian cyber attacker activity with a major improved detection and response capabilities. The number of successful high and critical severity incidents plummeted over the period since the war commenced. The SSSCIP attributes this success directly to the 'coordinated work' of a fused ecosystem of government, military, private sector, and civil society actors [35].

This integration was facilitated by international frameworks such as The Tallinn Mechanism, a coalition of allies which has coordinated civilian cyber capacity building since its founding in 2023 [36]. The value of this public-private fusion is demonstrated by a 2025 advisory in which U.S., UK, and international cyber authorities provided detailed analysis of Russian GRU cyber operations targeting defense logistics, leveraging insights from government intelligence and

private sector partners to enable network defenders to identify and mitigate these threats globally [37].

Legal foundations for such integration were laid in the Law on National Security of Ukraine [38] and strengthened in the National Cybersecurity Strategy 2021 [39], which explicitly recognized civil society and private-sector roles in national resilience. The 2021 National Cybersecurity Strategy (Decree No. 447/2021), assigned clear roles to government, private sector, and civil society actors in resilience, public-private partnership, and legal regulation. The National Coordination Center / State approach also includes metrics for success and public reporting.

Table 2.

Registered cyber incidents prior to and following the full-scale invasion, 2021-2024

Year	Total Registered Cyber Incidents	Critical & High-Level Incidents	Year-on-Year Change (Critical/High)	Implication
2021	1,350	403	—	Baseline year prior to full-scale invasion.
2022	2,194	1,048	+160%	Massive spike in severe attacks following the full-scale invasion.
2023	2,543	367	-65%	Drastic improvement in resilience; severe incidents plummet despite higher total volume.
2024	4,315	59	-84%	Sustained and accelerating defensive effectiveness against escalating attacks.

Source: War and Cyber, Three Years of Struggles and Lessons for Global Security (SSSCIP, 2025).

These frameworks enabled rapid mobilization of civilian expertise while preserving state oversight [40]. International partnerships with allied intelligence and private firms further amplified capabilities, creating a distributed innovation network that adapts faster than traditional bureaucracies especially to detect and mitigate Russian APT activity.

Organizational Innovation Under Pressure

Ukraine's model reflects democratic resilience under existential threat. Offensively, civilian groups such as the IT Army, Cyber Resistance, and the Cyber

Community for Free Ukraine evolved from ad hoc hacktivism into semi-coordinated auxiliaries, providing both cyber intelligence and cyber sabotage capability [23]. Reinforced by institutional innovations such as the Ministry of Digital Transformation (est. 2019) and state–civil society initiatives like the official establishment of the IT Army of Ukraine, which mobilized thousands of volunteer hackers into a coordinated auxiliary force [41]. These mechanisms illustrate how democracies can mobilize latent capacity in crises, though they also raise long-term questions about sustainability, security vulnerabilities,

Conversely, while Russia possesses organisations like the SVR, GRU and FSB that have demonstrated technically advanced cyber capabilities, its overall operational effectiveness suffers from institutional constraints. Competing intelligence agencies guard proprietary tools and resist integration with military operations [29; 30]. These rivalries, rooted in Putin's political system, impact the flow of time-sensitive intelligence to the battlefield. The result is cyber operations that are sophisticated in design but slow to adapt. Ukraine's horizontally integrated model emphasizes speed, flexibility, and continuous learning. These qualities consistently offset Russia's resource superiority.

The organizational lesson extends beyond Ukraine. NATO allies face the challenge of building accountable yet flexible structures that can integrate public, private, and civil society capacities. The UK's 2025 Strategic Defence Review acknowledges this need, calling for "breaking down barriers between individual Services, between the military and the private sector, and between the Armed Forces and wider society" [42]. While replication of Ukraine's model may be difficult in peacetime, its core principles—horizontal integration, civil society engagement, and adaptive institutional design—offer valuable guidance. Ukraine's own Cybersecurity Strategy 2021 [39] and the Concept for the Development of the Security and Defense Sector of Ukraine [43] highlight these priorities, providing frameworks that allies can study as they adapt democratic institutions to the digital battlefield.

Lesson 2: The Operationalization of Cyber for Combined Arms Warfare

The second major innovation lies in bridging the traditional gap between cyber operations and battlefield functions. Cyber is no longer confined to strategic intelligence gathering but is increasingly integrated into both strategic and tactical operations. This marks a doctrinal evolution: cyber is no separate or isolated domain but, under the right conditions, an increasingly productive element of combined arms warfare.

From Strategic to Tactical Cyber Operations

Traditional cyber operations have historically pursued strategic objectives—long-term intelligence collection, major infrastructure disruption, or high-level political influence. The war in Ukraine has demonstrated cyber's evolution into direct battlefield support, fundamentally expanding operational applications and compressing decision cycles [44].

Russia's deployment of the Infamous Chisel malware, which tracked Ukrainian troop positions via Android devices, that enabled near real-time artillery targeting [45] is the most high profile example; illustrating what Maschmeyer [17] terms "cyber persistence": sustained access that delivers continuous operational support and as Smeets [18] argues cyber achieves strategic value only when integrated with broader military campaigns.

The Fusion Model

The fusion of cyber and kinetic operations is the most direct outcome of combat-driven integration. Faced with the immediate need to survive, Ukraine's military and security services were compelled to break down traditional silos and embed cyber capabilities at the tactical edge, a process that would have potentially taken years under peacetime conditions.

Ukraine's offensive cyber power stems from a two-tier model combining state institutions with civilian volunteers and partners. Military intelligence (HUR) conducts APT-level espionage against Russian ministries and defense firms, while civil groups generate tactical intelligence through social media monitoring and open-source analysis as well as providing both standalone cyber sabotage operations and ones integrated into broader kinetic action [28].

Civilian networks are now assessed to be able to move information from collection to battlefield use within hours—an agility traditional intelligence cycles cannot match [46]. Coordination between official and unofficial actors maintains security while maximizing information flow. This fusion has enabled cyber strikes on Russian command software and the disruption of drone control systems [47], demonstrating the potential of this emergent novel "whole-of-nation" model of cyber-enabled warfare.

Unlike Russia's early reliance on large-scale destructive operations for psychological shock [29], Ukraine emphasizes precision. Its cyber actions support drone strikes, disable surveillance systems, and disrupt communications in coordination with kinetic operations [23]. This approach reflects both necessity—Ukraine cannot match Russia's scale—and strategy: synchronized cyber support provides more battlefield advantage than isolated cyber sabotage. For NATO, the lesson is clear: cyber power lies less in spectacular, standalone attacks than in timely, integrated effects.

The Warfighter's New Reality

The integration of cyber into routine military operations represents a fundamental shift in warfighting requirements. Future leaders must understand digital intelligence collection—its strengths and limitations—alongside cyber threat mitigation and information warfare as core competencies, not specialist functions.

Commanders must also incorporate digital offense and defense into decision-making processes. At the same time, civil–military cooperation introduces challenges of coordination, security, and command authority. Ukraine has improvised solutions under wartime pressure; NATO allies face the harder task of institutionalizing them in peacetime. As RUSI and the UK's National Cyber Force

argue, Western militaries require “new thinking” that embeds offensive and defensive cyber into doctrine rather than treating them as separate technical functions [48].

Lesson 3: The Information Warfare Crisis

Ukraine’s third lesson exposes the structural domain where democracies remain most vulnerable: information warfare. Russia’s coordinated disinformation campaigns have consistently shaped perceptions, weakened morale, and influenced political debates across borders. By contrast, Western responses are fragmented, scattered across agencies with overlapping mandates and limited resources.

The Undefended Domain

Of Rid’s three cyber categories, subversion has been Russia’s most effective. Ukraine has faced these operations both tactically—targeting frontline units with demoralizing narratives, falsified battlefield footage, and fake surrender messages—and strategically, through campaigns designed to erode foreign support for aid and to polarize allied societies [46; 49; 50].

Detailed case studies of these campaigns have documented their specific narratives, such as framing the conflict as a necessary "denazification" of Ukraine and a proxy war against the West, and have analyzed their measurable impacts on shaping public perception [49]. Russian operations systematically exploit the structural openness of democratic media systems, using social media platforms as central propaganda tools to wage information war in the post-truth era [51]. Their campaigns are designed to move faster than the slow, siloed responses of most Western institutions.

This vulnerability is institutional, not technological. Russia embeds the cognitive domain in its national security strategy, while democratic states divide responsibilities between militaries, intelligence agencies, civilian regulators, and private platforms. The result is slow detection, unclear authority, and inconsistent messaging—conditions adversaries exploit to gain initiative.

Analysis of available intelligence reporting reveals the vast complexity of these efforts. Recorded Future has documented dozens of major Russian influence campaigns since 2022. These include Operation Undercut (targeting Western military aid debates) [52], Operation Overload (impersonating media to manipulate the 2024 U.S. election discourse) [53], and coordinated efforts against German [54] Romanian, and Moldovan [55] elections.

The volume of output suggests subversion may represent a larger share of Russia's overall cyber effort than other types of cyber operations, a strategic choice that exploits democratic vulnerabilities more effectively than technical attacks. As the reporting illustrates, Russia operates multiple parallel influence networks, each running dozens of simultaneous narratives across hundreds of platforms, representing thousands of daily posts.

Ukraine's Counter-Innovation

Despite being under constant attack, Ukraine has developed a model for counter-disinformation rooted in authenticity, devolved coordination, and speed [56; 57]. Rather than attempting to match Russia's "firehose of falsehood," Ukraine focuses on verified content [58]: transparent updates from military commands, documentation of battlefield outcomes, and rapid correction of fabrications.

This rapid, integrated response was most evident during the successful Kharkiv offensive in late 2022 [59; 60]. As Ukrainian forces made rapid gains, Russia's cyber information operations attempted to sow confusion and panic, spreading disinformation that their retreat was a feigned withdrawal designed to lure Ukrainian troops into a trap [61]. In a clear example of combat-driven integration, Ukraine's Ministry of Defense, supported by civilian volunteers and open-source intelligence groups, immediately countered this narrative [59]. They published real-time, geolocated video evidence of a full-scale Russian retreat, directly undermining the psychological operation and maintaining operational momentum [62]. The speed and unity of this response—coordinating military action with information defense—showcased how Ukraine's institutional agility defeats Russia's information warfare at the tactical level [56].

Table 3.

Kharkiv Offensive – Russian Narratives versus Ukrainian Counter-Narratives

	Russian Narrative	**Ukrainian Counter-Narrative**
Narrative Title	'Feigned Retreat' / 'Regrouping'	Strategic Feint / Defensive Breakthrough / Liberation
Source	Kremlin, Ministry of Defense	Ukrainian Military Command, OSINT community, Civil Society
Objective	Salvage political credibility, minimize military defeat.	Create strategic military advantage, document war crimes, expose Russian losses.
Analysis	Weak, reactive, incoherent, and contradicted by on-the-ground reality.	Proactive, multi-faceted, fact-based, and highly effective due to synergy between military and civilian actors.

For decades, open societies have struggled with information warfare, often resorting to a reactive, fact-checking paradigm. Ukraine, however, introduced a new model. Rather than simply debunking falsehoods, Kyiv's strategy leveraged a cohesive national narrative centered on authenticity and shared values. This approach demonstrates that in the information age, the most powerful defense against a

'firehose of falsehood' is not a competing propaganda machine, but a trustworthy and coordinated national voice that empowers civil society to become a frontline of truth.

Institutional coordination is a central element of Ukraine's information warfare strategy, which operates under the strategic oversight of the Centre for Countering Disinformation (CCD), a body under the National Security and Defense Council [63]. This approach is not a centralized propaganda machine but rather a model of decentralized execution that draws on civil society, diaspora communities, and volunteer networks. For example, independent media and organizations like StopFake and Detector Media carry out crucial fact-checking and investigative work, while groups such as the PR Army mobilize communication specialists to shape international narratives [64]. The Ministry of Digital Transformation also contributes by supporting monitoring efforts and mobilizing volunteers, deliberately linking operational success to narrative impact. This framework is supported by the 2021 National Cybersecurity Strategy [63] and its implementing decrees.

The CCD and other coordinating bodies operate within a policy framework buttressed by the 2021 Strategy and implementing decrees (Decree No. 447/2021), which grant RNBO and associated agencies clearer authorities for coordination and measurement of outcomes. In addition, Ukraine's implementation plan for the 2021 Strategy included public-private partnership mechanisms and civil society mobilization for information monitoring, reflecting both tactical responses (to fake battlefield narratives) and strategic communications tasks.

This approach has yielded tactical and strategic results. At the tactical level, Ukraine has countered false surrender messages and disinformation designed to paralyze units. At the strategic level, coordinated messaging—through authentic combat footage, international briefings, and carefully timed campaigns—has bolstered public resilience and sustained international support albeit acknowledging the difficulties.

The Western Institutional Gap

In contrast, Western counter-disinformation frameworks remain fragmented. Military psy-ops focus outward, intelligence services are constrained domestically, civilian regulators lack speed and resources, and technology platforms set their own standards based on commercial logic. Even when disinformation campaigns are identified, responses are delayed or inconsistent. Recent cases in Europe—including election interference in Romania and Germany, and riot-triggering campaigns in the UK—show how adversaries exploit these institutional weaknesses.

Unlike espionage or sabotage, information warfare exploits inherent features of democratic societies: openness, pluralism, and free expression. Russian operations have degraded Ukrainian morale, influenced foreign parliamentary votes, and polarized allied societies—all at a fraction of the cost of conventional operations. These effects are enduring and politically consequential, making this domain the most strategically dangerous. Institutional fragmentation ultimately creates a governance gap that adversaries can systematically exploit, turning the inherent strengths of an open society into a key vulnerability in the information domain.

Institutional Adaptation Will Be Required

Ukraine demonstrates that democracies can respond effectively without abandoning democratic principles, but only if they build institutions with clear authority and rapid decision-making. The CCD offers one model: a central hub for coordination that empowers distributed execution across government, civil society, and private actors. Pre-established procedures for rapid response are essential, since bureaucratic delays cede the initiative to adversaries.

Other democracies can draw on lessons from Ukraine's experience both confirming and extending these cases: like Estonia after 2007, it institutionalized whole-of-society cyber defense [65]; like Israel, it integrated cyber directly into warfighting functions [66]; and like Taiwan [67], it leverages volunteer-based counter-disinformation networks.

The common thread between all these experiences against authoritarian digital subversion is that agility, authenticity, and integration matter more than scale. Ukraine's experience proves that even under sustained assault, coordinated democratic responses can contest the information domain. The question for Western allies is whether they can institutionalize similar reforms in peacetime. Ultimately, Ukraine's experience demonstrates that the three critical lessons—organizational agility, cyber-kinetic integration, and institutionalized information defense—are all powerful examples of combat-driven integration.

IV. Strategic Implications for NATO and Allied States

Ukraine's wartime innovations offer lessons that extend well beyond the current conflict. For NATO and partner nations, the central message is clear: institutions must adapt faster than technology. Scholars of military innovation have long argued that organizational design and political context shape outcomes as much as technical capacity [12; 68]. Ukraine's experience confirms this insight, demonstrating that institutional agility, cyber–warfighter integration, and narrative coherence can offset the numerical and technical advantages of an adversary [9; 17]. For allies, the challenge is whether these insights can be internalized in peacetime—before a future confrontation forces adaptation under fire.

1. The Organizational Imperative

Ukraine's horizontal integration of government, civil society, and the private sector provides a model for defensive and offensive cyber operations as well as democratic resilience. This approach enabled speed, creativity, and continuity despite sustained cyberattacks and subversion. In contrast, many Western defense systems remain structured around siloed bureaucracies and slow approval chains, a problem long identified in comparative studies of national security decision-making [69]. Allies need to understand Ukraine's governance model as described in *National Cybersecurity Governance: Ukraine* [70], where risk-based, legally underpinned coordination among state bodies, volunteer actors, and civil society is institutionalized, including predefined metrics and accountability.

The implication is that allied states must reconsider how to institutionalize "whole-of-society" cyber structures that remain accountable but flexible. Estonia's

Cybersecurity Strategy 2024–2030 illustrates such thinking, emphasizing national cyber hygiene programs and citizen engagement [71]. For larger NATO members though achieving comparable integration will require not only technical investment but also new legal frameworks, trusted information-sharing mechanisms, and culturally embedded norms of collaboration at a whole different scale.

Alternative explanations merit consideration

One is Western intelligence and technical support—from real-time Allied threat intelligence, Microsoft's telemetry access, Amazon's Cloud Services, Palantir's analytics to allied cyber command support. This undoubtedly amplified Ukraine's capabilities. However, this support actually reinforces rather than contradicts the organizational thesis.

Multiple states — including Georgia after 2008, Moldova since 2022, and even NATO allies such as the Baltic states and Poland — have received similar, albeit on a smaller scale of, Western assistance, ranging from NATO trust funds to U.S. Cyber Command "hunt forward" missions [72; 73] and Microsoft threat intelligence support [74; 75; 34]. Yet none have achieved Ukraine's level of real-time integration across military, government, private, and civil society actors.

This contrast reinforces the organizational thesis: external support is necessary but not sufficient without institutions capable of synthesizing it into operational effectiveness. Ukraine's ability to synthesize diverse streams of support into operational coherence demonstrates that institutional design determines whether external support translates into operational effectiveness [28]. Resources without integration structures and capabilities remain tactically useful but strategically limited.

2. The Military Transformation Challenge

Cyber effects in Ukraine are not strategic abstractions but are now tactical enablers: disrupting command systems, guiding artillery, protecting logistics, and shaping deception operations [76]. This integration was possible because cyber activities were fused into daily combat planning rather than treated as a separate technical specialty. For NATO militaries, this raises hard questions about force design and doctrine.

Maschmeyer’s concept of “cyber persistence” highlights the importance of continuous operational engagement over singular strategic blows [17], a lesson reinforced by Ukraine’s experience. Yet most allied doctrines still compartmentalize cyber, placing expertise within national-level commands that struggle to influence battalion-scale operations. France’s 2022 National Strategic Review, shaped by the war in Ukraine, called for “profound change” in military thinking to incorporate hybrid realities, and the establishment of COMCYBER represents one effort at integration [77]. Still, without retraining officers, restructuring organizations, and accelerating procurement cycles, cyber will remain underutilized at the tactical edge.

3. The Information Warfare Crisis

The conflict has also exposed that democracies remain dangerously vulnerable in the information domain. Russia's "firehose of falsehood" strategy [78] has exploited bureaucratic divides across Western institutions, while Ukraine countered with a coherent and authentic narrative that galvanized domestic and international support [79]. The institutional gap is stark: militaries own psychological operations mandates, civilian agencies manage communications, and private platforms control much of the information environment.

For NATO members, the lesson is that disinformation cannot be relegated to the periphery—it is a central battlefield shaping legitimacy and cohesion. The strategic challenge is to build mechanisms for coordinated, rapid response that respect democratic freedoms. Without such innovation, authoritarian adversaries will continue to exploit speed, ambiguity, and societal division.

The Institutional Reform Imperative

The broader implication is that the window for learning is finite. As scholars of security institutions note, moments of crisis often open rare opportunities for structural reform [80]. Ukraine has shown how a democratic society under existential threat can innovate rapidly to outpace a larger authoritarian adversary. But allies cannot assume these lessons will automatically transfer into their own systems. Without deliberate reform, bureaucratic inertia risks leaving NATO states unprepared for the next conflict in which cyber, conventional, and informational tools converge. The strategic imperative, then, is not simply to admire Ukraine's resilience but to translate its experience into institutional change—before another crisis forces the same reckoning under less favorable conditions.

The transferability challenge is substantial. Peacetime democracies face structural barriers to replicating Ukraine's model: legal constraints on civil-military integration, privacy protections limiting information sharing, commercial interests diverging from security priorities, and the absence of existential threat to motivate coordination. Yet elements can be adapted: pre-authorized emergency protocols, regular joint exercises, legal frameworks for crisis coordination, and cultural preparation through education and awareness programs.

Questions about sustainability are also partially answered by duration—Ukraine's model has now operated for over three years, evolving from emergency improvisation to institutionalized practice. The relative stabilization of front lines since late 2022 has allowed refinement of processes and formalization of initially ad-hoc arrangements. However, long-term sustainability remains uncertain, particularly regarding volunteer motivation, security risks from distributed operations, and post-conflict normalization.

V. Three Critical Questions

Ukraine's experience raises critical questions that extend beyond its borders. These are not only strategic puzzles for Western defense communities but also tests of whether democratic states can adapt fast enough to counter authoritarian cyber

power including when combined with military force. Three questions in particular deserve attention.

First, how should democratic societies organize for cyber conflict?

Ukraine's success suggests that agility emerges from horizontal integration—government, civil society, and private actors collaborating in real time. This contrasts with the centralized, hierarchical traditions of most Western militaries. Some allies are beginning to adapt; Estonia's Cybersecurity Strategy 2024–2030 reflects a "whole-of-country" approach, emphasizing national cyber hygiene programs and citizen awareness to address vulnerabilities exposed by Ukraine's experience [71]. Finland's 2024–2035 strategy likewise stresses unified public–private action as part of comprehensive security [81].

These echo Ukraine's fusion of state capacity with societal resilience, though whether they can be institutionalized in peacetime without the urgency of war remains uncertain. Yet this civilianization of cyber conflict also raises profound ethical and legal questions. The integration of civilian hackers blurs combatant/non-combatant distinctions fundamental to international law [82]. While Ukraine's approach has proven operationally effective, it risks setting precedents that authoritarian regimes could exploit to justify targeting civilian technical infrastructure and personnel.

This question must be owned jointly by national cyber agencies, ministries of defense, NATO and other international agencies, since it implicates both operational design and legal frameworks governing armed conflict.

Second, how should militaries embed cyber at the tactical edge?

In Ukraine, cyber operations now influence artillery accuracy, drone reconnaissance, and battlefield deception, becoming woven into daily combat [83]. Many Western doctrines still treat cyber as a distinct strategic function, risking the loss of its operational potential. France's 2022 National Strategic Review explicitly drew lessons from Ukraine, calling for “profound change” in military thinking to integrate hybrid realities [76]. Its creation of the Cyber Defence Command (COMCYBER) represents a move toward formal cyber–warfighter integration [84]. But the central challenge remains cultural: retraining personnel, restructuring organizations, and ensuring cyber effects are understood and usable at the battalion and company levels, not just at national command.

Answering this question falls squarely on armed forces and military education systems: general staffs, doctrine centers, and professional military schools must make cyber literacy an operational norm rather than a specialist enclave.

Third, how should democracies defend against information warfare?

Russia has consistently exploited Western fragmentation with volume-driven disinformation campaigns, while Ukraine countered with a unified and authentic narrative. Yet information warfare has also been a live battlefield problem. Russian units have deployed psychological operations in occupied territories, spread false orders to Ukrainian troops, and flooded frontline Telegram channels with disinformation to sow confusion and erode morale.

Ukraine responded by tightly coordinating strategic communications across government and military channels, ensuring that clear, trusted messaging reached

both domestic and international audiences. Initiatives like the Centre for Strategic Communications and Information Security (StratCom) and military-linked Telegram channels provided rapid corrections of false narratives, while OSINT and volunteer groups exposed Russian fabrications in near real time.

Liberal democracies remain vulnerable because of their open information environments and bureaucratic divides. France's 2022 Review emphasized "moral rearmament," recognizing that public trust and societal cohesion are as critical as technical defenses [76]. The pressing challenge is to build mechanisms for coordinated, rapid response that respect freedom of expression while also delivering timely counteraction. Even defining success metrics in this domain remains unresolved.

This question must be addressed by a coalition of actors: strategic communications agencies, media regulators, civil society fact-checking networks, military information operations units, and technology platforms. Governments alone cannot solve it.

Together, these questions highlight both the promise and limits of adaptation so far. Allies are beginning to act—through strategy documents, new commands, and public–private initiatives—but Ukraine's experience demonstrates that more profound institutional change will be required. Democratic states must rethink how they mobilize society, integrate technology, and defend the information space. Ukraine has shown what is possible under existential pressure; the challenge for its partners is to translate those lessons into durable reforms before the next conflict tests their systems under less favorable conditions.

VI. Conclusion: The Window for Learning

Ukraine’s transformation from cyber victim to cyber power demonstrates that organizational design and institutional agility—not raw technical capacity—determine effectiveness in cyber conflict. By integrating civil society, private sector, and state resources into a coherent ecosystem, Ukraine has turned vulnerability into advantage, offering a rare living laboratory for understanding cyber-enabled warfare.

Three broad lessons emerge: horizontally integrated institutions, the embedding of cyber in conventional warfighting, and coordinated responses to information warfare. Together, these insights reinforce an adaptation primacy thesis—that in protracted cyber conflict, organizational adaptability matters more than initial capability. While this principle is not new, Ukraine provides the first extended empirical case in the cyber domain, demonstrating how democratic societies can operationalize it under wartime conditions.

This study also identifies combat-driven integration as a distinct mechanism of institutional adaptation, whereby existential conflict accelerates the fusion of cyber capabilities with military and civil structures beyond what peacetime reform could achieve. While Ukraine’s wartime innovations provide a powerful template for institutional agility, a critical long-term question remains for Western allies: the sustainability of such a model. Can a state maintain a high level of national unity and a robust, volunteer-driven cybersecurity ecosystem in peacetime, when a clear

and present threat is absent? The collective action and decentralized resilience observed in Ukraine are products of an existential crisis, and the challenge for allied nations is to translate these wartime necessities into enduring, peacetime institutional structures that are not dependent on a shared sense of immediate danger.

The opportunity is clear: Ukraine shows that democracies can innovate under pressure to offset authoritarian advantages. The urgency is also clear: unless allies translate these lessons into institutional reform, future conflicts may expose the same vulnerabilities. The strategic imperative is not merely to admire Ukraine's resilience but to translate its experience into institutional change—before another crisis forces the same reckoning under less favorable conditions. This is particularly critical as emerging technologies like artificial intelligence threaten to compress decision cycles and automate elements of cyber conflict, potentially accelerating the pace of future wars and conflict.

A "post-Ukraine" model of cyber power will not be defined by any single set of technologies, but by the agility of its human and institutional networks. The ability to rapidly integrate AI-powered systems, crowd-sourced intelligence, and dynamic narrative responses will be a direct function of a state's organizational design—the very lessons Ukraine has so powerfully demonstrated on a sustained, national scale. The question for Western allies is whether they can embed these principles into their own systems and doctrine in peacetime, ensuring they are prepared for a future where adaptability, not just capability, will determine the victor.

Appendix A: Methodology Note

The conclusions of this analysis are subject to several constraints. First, because of reliance on open sources and not classified sources, there are inherent data gaps. Many cyber operations, especially successful ones, remain confidential due to operational security concerns not least during an ongoing conflict. Second, a potential systematic bias exists due to the different information disclosure practices of Ukraine and Russia regarding cyber activities. Finally, this report examines an active and rapidly evolving conflict, meaning new information is always emerging. As a result, our conclusions may need to be updated as the situation develops.

Despite these limitations, the large volume of open-source intelligence available on Russo-Ukrainian cyber activity provides a strong foundation for a meaningful analysis. These insights are best understood when viewed within the context of ongoing operations and the continuous evolution of institutional practices.

References

1. Mastalski M.C. Russia's Implementation of Hybrid Warfare: Estonia ('07), Georgia ('08), Crimea ('14). *Wild Blue Yonder*. Air University. Washington. 2021. 27 April. URL: https://www.airuniversity.af.edu/Wild-Blue-

Yonder/Articles/Article-Display/ Article/2582363/russias-implementation-of-hybrid-warfare-estonia-07-georgia-08-crimea-14/
2. Cyberattacks likely to rise in wake of Ukraine war: What Estonia learnt from Web War One. *Euronews*. 2022. 26 May. URL: https://www.euronews.com/next/2022/05/26/cyberattacks-likely-to-rise-in-wake-of-ukraine-war-this-is-what-estonia-learnt-from-web-wa
3. Otto E. Russian Cyberattacks Are Strengthening Ukraine. *CEPA*. Washington. 2024. 14 August. URL: https://cepa.org/article/russian-cyberattacks-are-strengthening-ukraine/
4. Blessing J. Where is Russia's cyber blitzkrieg? *The Hill*. 2022. 24 March. URL: https://thehill.com/opinion/cybersecurity/599599-where-is-russias-cyber-blitzkrieg/
5. Gartzke E., Lindsay J.R. Thermonuclear cyberwar. *Journal of Cybersecurity*. 2017. Vol. 3, No. 1. P. 37-48.
6. Libicki M.C. Conquest in Cyberspace: National Security and Information Warfare. Cambridge : Cambridge University Press, 2007.
7. Borghard E.D., Lonergan S.W. The logic of coercion in cyberspace. *Security Studies*. 2017. Vol. 26, No. 3. P. 452-481. URL: https://doi.org/10.1080/09636412.2017.1306396
8. Kello L. The meaning of the cyber revolution: Perils to theory and statecraft. *International Security*. 2013. Vol. 38, No. 2. P. 7-40.
9. Rid T. Cyber war will not take place. *Journal of Strategic Studies*. 2011. Vol. 35, No. 1. P. 5-32.
10. The head of GCHQ says Vladimir Putin is losing the information war in Ukraine. *The Economist*. 2022. 18 August. URL: https://www.economist.com/by-invitation/2022/08/18/the-head-of-gchq-says-vladimir-putin-is-losing-the-information-war-in-ukraine
11. Posen B.R. The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars. Ithaca : Cornell University Press, 1984.
12. Rosen S.P. Winning the Next War: Innovation and the Modern Military. Ithaca : Cornell University Press, 1991.
13. Avant D.D. Political Institutions and Military Change: Lessons from Peripheral Wars. Ithaca : Cornell University Press, 1994.
14. Cote O.R. The politics of innovative military doctrine: The U.S. Navy and fleet ballistic missiles. *Security Studies*. 2000. Vol. 9, No. 3. P. 50-89.
15. Zhora V. Ukraine repels Russian cyberattacks, says SSSCIP. *Kyiv Independent*. 2022. 1 March. URL: https://kyivindependent.com/ukraine-repels-russian-cyberattacks-says-ssscip

16. Buchanan B. The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics. Cambridge : Harvard University Press, 2020.
17. Maschmeyer L. The subversive trilemma: Why cyber operations fall short of expectations. *International Security*. 2021. Vol. 46, No. 2. P. 51–90.
18. Smeets M. The strategic promise of offensive cyber operations. *Strategic Studies Quarterly*. 2018. Vol. 12, No. 3. P. 90-113.
19. Greenberg A. The untold story of NotPetya, the most devastating cyberattack in history. *Wired*. San Francisco. 2018. 22 August. URL: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
20. Varvitsioti A., Cerulus L., Forgey Q. Russian invasion of Ukraine could redefine cyber warfare. *Politico*. 2022. 28 January. URL: https://www.politico.eu/article/russia-ukraine-war-cyber-attacks-invasion/
21. Otwinowski M., Khoo C. The Russia-Ukraine Conflict from 2014 to 2023 and the Significance of a Strategic Approach to Cyber Defence. *ACIG Journal*. 2023. URL: https://www.acigjournal.com/The-Russia-Ukraine-Conflict-from-2014-to-2023-and-the-Significance-of-a-Strategic,184308,0,2.html
22. Report on Cyber Threats for 2023. *SSSCIP* (State Service of Special Communications and Information Protection of Ukraine). Kyiv, 2023.
23. Kirichenko D. Ukraine's IT Army is waging a crowdsourced cyber war against Russia. *Small Wars Journal*. 2025. 24 March. URL: https://smallwarsjournal.com/2025/03/24/ukraines-it-army-is-waging-a-crowdsourced-cyber-war-against-russia/
24. Santora M., Higgins A. 'IT Army of Ukraine': Hundreds of Thousands Volunteer to Fight Russia Online. *The New York Times*. 2023. 20 February. URL: https://www.nytimes.com/2023/02/20/world/europe/ukraine-it-army-russia-cyber.html
25. Ukraine's cyber chief on Russian hackers' shifting tactics, US cyber aid. *The Record*. Washington. 2024. December. URL: https://therecord.media/ukraine-cyber-chief-on-russia-hacks-us-aid
26. Cyber-Attacks on Ukraine Surge 123%, But Success Rates Plummet. *Infosecurity Magazine*. London. 2025. 2 June. URL: https://www.infosecurity-magazine.com/news/cyberattacks-ukraine-surge-success/
27. Ukraine Faces 12 Major Cyber Incidents Daily – SSSCIP Warns. *Odessa Journal*. 2025. URL: https://odessa-journal.com/at-infosec-ukraine-2025-staggering-statistics-on-cyber-incidents-in-ukraine-were-revealed
28. Dixon W. Ukraine as the cyber Spanish Civil War. *Ukrainian Policymaker*. Kyiv. 2025. Vol. 16. P. 55-73. URL: https://doi.org/10.29202/up/16/4

29. Giles K. Russian Cyber and Information Warfare in Practice. London : Chatham House, 2023.
30. Sherman J. Unpacking Russia's cyber nesting doll. *Atlantic Council*. Washington. 2025. 20 May. URL: https://www.atlanticcouncil.org/content-series/russia-tomorrow/unpacking-russias-cyber-nesting-doll/
31. Goldsmith S., Eggers W. D. Governing by Network: The New Shape of the Public Sector. Washington : Brookings Institution Press, 2004.
32. Huxham C., Vangen S. Managing to Collaborate: The Theory and Practice of Collaborative Advantage. London : Routledge, 2005.
33. Defending Ukraine: Early lessons from the cyber war. *Microsoft on the Issues*. Redmond. 2022. 22 June. URL: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/
34. Microsoft launches new European Security Program. *Microsoft On The Issues*. 2025. 5 June. URL: https://blogs.microsoft.com/on-the-issues/2025/06/04/microsoft-launches-new-european-security-program/
35. War and Cyber, Three Years of Struggles and Lessons for Global Security. *SSSCIP* (State Service of Special Communications and Information Protection of Ukraine). Kyiv, 2025.
36. UK Foreign, Commonwealth & Development Office (FCDO). Joint statement on the first anniversary of the Tallinn Mechanism. *UK Government*. London. 2024. 15 February. URL: https://www.gov.uk/government/news/joint-statement-on-the-first-anniversary-of-the-tallinn-mechanism
37. CISA et al. Russian GRU Cyber Actors Target Defense Logistics. *Cybersecurity Advisory*. Washington. 2025. 21 May. URL: https://media.defense.gov/2025/May/ 21/2003719846/-1/-1/0/CSA_RUSSIAN_GRU_TARGET_LOGISTICS.PDF
38. Закон України "Про національну безпеку України". Док. 2469-VIII від 21.06.2018. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
39. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України". Указ Президента України. Док. 447 від 26.08.2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12
40. Renden-Katolik A. The IT Army of Ukraine. *Center for Strategic and International Studies*. Washington. 2023. 15 August. URL: https://www.csis.org/blogs/strategic-technologies-blog/it-army-ukraine
41. Захист критичної інфраструктури України від кіберзагроз. *DefTech.dou.ua*. 2024. 18 квітня. URL: https://dou.ua/forums/topic/48403/
42. The Strategic Defence Review 2025 - Making Britain Safer: Secure at Home, Strong Abroad. *UK Government*. London. 2025. URL:

https://www.gov.uk/government/publications/the-strategic-defence-review-2025-making-britain-safer-secure-at-home-strong-abroad
43. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України". Указ Президента України. Док. 392/2020, редакція від 07.01.2025. URL: https://zakon.rada.gov.ua/laws/show/392/2020#n12
44. Black D. Russia's cyber campaign shifts to Ukraine's frontlines. *Royal United Services Institute*. London. 2024. 2 July. URL: https://www.rusi.org/explore-our-research/publications/commentary/russias-cyber-campaign-shifts-ukraines-frontlines
45. NCSC et al. Infamous Chisel – Sandworm's Android malware used against Ukraine. *NCSC*. Ottawa. 2023. September. URL: https://www.cyber.gc.ca/en/news-events/joint-report-new-russian-malware-campaign-targeting-ukrainian-military
46. How Ukraine is waging information warfare to outwit Russians. *The Times*. 2024. 15 October. URL: https://www.thetimes.com/world/russia-ukraine-war/article/how-ukraine-is-waging-information-warfare-to-outwit-russians-5zn3fxlmm
47. Ukrainians hacked Russian program for drone control – DIU. *UNN*. 2024. 8 February. URL: https://unn.ua/en/news/ukrainians-hacked-russian-program-for-drone-control-diu
48. RUSI & NCF. Encouraging New Thinking on Offensive Cyber Operations. *RUSI*. 2025. URL: https://www.rusi.org/explore-our-research/publications/commentary/encouraging-new-thinking-offensive-cyber-operations
49. Barić, M., Burić, I. Case Study of the Russian Disinformation Campaign During the War in Ukraine Propaganda Narratives, Goals and Impacts. *National Security and the Future*. Zagreb. 2023. Vol. XXIV, No. 3. P. 497-514. URL: https://www.nsf-journal.hr/nsf-volumes/case-studies/id/1471
50. Danchenkova O. Ukraine's hard-won approach to strategic communications and counter-disinformation: Lessons for Europe and beyond. *Tech Policy Press*. Washington. 2025. 12 March. URL: https://www.techpolicy.press/ukraines-hardwon-approach-to-strategic-communications-and-counterdisinformation-lessons-for-europe-and-beyond/
51. Ogunyemi O. Digital Media and War: Social Media as a Propaganda Tool for the Russia-Ukraine Conflict in the Post-truth Era. *The Palgrave Handbook of Media and Communication Research in Africa*. Cham : Palgrave Macmillan, 2023. URL: https://www.researchgate.net/publication/368496869_Digital_Media_and_War_Social_Media_as_a_Propaganda_Tool_for_the_Russia-Ukraine_Conflict_in_the-Post-truth_Era

52. “Operation Undercut” Shows Multifaceted Nature of SDA's Influence Operations. *Recorded Future*. Insikt Group. Boston. 2024. 16 November. URL: https://go.recordedfuture.com/hubfs/reports/TA-RU-2024-1126.pdf
53. Operation Overload Impersonates Media to Influence 2024 US Election. *Recorded Future.* Insikt Group. Boston, 2024. 15 May. URL: https://www.recordedfuture.com/research/operation-overload-impersonates-media-influence-2024-us-election
54. Stimmen aus Moskau: Russian Influence Operations Target German Elections. *Recorded Future.* Insikt Group. Boston, 2024. 28 August. URL: https://www.recordedfuture.com/research/stimmen-aus-moskau-russian-influence-operations-target-german-elections
55. Cojocaru A., Cárpenco A. Targeted disruption: Russian interference in the 2024 elections of Moldova, Romania, and Georgia. *Politics & Geopolitics*. 2024. URL: https://politicsgeo.com/targeted-disruption-russian-interference-in-the-2024-elections-of-moldova-romania-and-georgia/
56. Mazarr M.J. Understanding Ukrainian Success in the Information War. *RAND Corporation*. 2024. URL: https://www.rand.org/pubs/research_reports/RRA2771-1.html
57. Zavadskyi Y. How Ukraine's Civil Society Battles Russia in the Information War. *Ukraïner*. Kyiv. 2023. URL: https://www.ukrainer.net/en/how-ukraine-s-civil-society-battles-russia-in-the-information-war/
58. Perrigo B. How Open-Source Intelligence is Helping Expose the Ukraine-Russia War. *Time*. 2022. URL: https://time.com/6150884/ukraine-russia-attack-open-source-intelligence/
59. Byshchenko O. Bombs and disinformation: Russia's campaign to depopulate Kharkiv. *Atlantic Council*. Washington. 2022. URL: https://www.atlanticcouncil.org/blogs/ukrainealert/bombs-and-disinformation-russias-campaign-to-depopulate-kharkiv/
60. Hlazkova S. Information Warfare in the Ukrainian-Russian War. *Academic Journal of the National Defense University of Ukraine*. Kyiv. 2022. Vol. 91, No. 4. P. 11-19.
61. Mitchell Institute Communications Team. Kharkiv Activists Fight for Truth Against Disinformation. *Mitchell Institute News*. Queen's University Belfast. 2024. URL: https://www.qub.ac.uk/Research/GRI/mitchell-institute/news/2024/kharkiv-activists-fight-for-truth-against-disinformation.html
62. Carter-Tanner D.H.C. The Ukrainian Kharkiv Counter-Offensive and Information Operations. *The Cove*. Canberra. 2023. URL: https://cove.army.gov.au/article/ukrainian-kharkiv-counter-offensive-and-information-operations

63. National Cybersecurity Strategy of Ukraine. *National Security and Defense Council of Ukraine*. Kyiv, 2021.
64. How Ukraine's civil society battles Russia in the information war. *Ukraïner*. Kyiv. 2025. 7 May. URL: https://www.ukrainer.net/en/how-ukraine-s-civil-society-battles-russia-in-the-information-war/
65. Pevkur H. Lessons from Estonia's Whole-of-Society Approach to Cyber Defense. *Digital Front Lines*. Tallinn, 2023.
66. Israel's National Cybersecurity and Cyberdefense Posture. *Cyberdefense Report*. CSS/ETH Zürich. 2020. URL: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf
67. Zhang L. How to Counter China's Disinformation Campaign in Taiwan. *Military Review*. 2020. Vol. 100, No. 5. P. 21-32. URL: https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/September-October-2020/Zhang-Disinformation-Campaign/
68. Cote O. R. The politics of innovative military doctrine: the U.S. Navy and Fleet Ballistic Missiles. Ph.D. Dissertation. Boston : Massachusetts Institute of Technology, 1996.
69. Allison G.T., Zelikow P. Essence of Decision: Explaining the Cuban Missile Crisis. Vol. 2. 2nd ed. N.Y. : Addison Wesley, Longman, 1999.
70. Davydiuk A., Potii O. National Cybersecurity Governance: Ukraine. *NATO Cooperative Cyber Defence Centre of Excellence*. Tallinn. 2024. URL: https://ccdcoe.org/uploads/2024/08/National-Cybersecurity-Governance_Ukraine_ Davydiuk_Potii_2024.pdf
71. Cybersecurity Strategy 2024-2030: Cyber-Conscious Estonia. *Ministry of Economic Affairs and Communications*. Government of Estonia. Tallinn. 2024. URL: https://www.justdigi.ee/sites/default/files/documents/2024-12/Cybersecurity%20strategy%202024–2030%20 Cyber-conscious%20Estonia.pdf
72. Cyber Command sent a 'hunt forward' team to help Lithuania harden its systems. *The Record*. Washington. 2023. 10 May. URL: https://therecord.media/cyber-command-sent-a-hunt-forward-team-to-help-lithuania-harden-its-systems
73. US, Canada sent cyber experts to Latvia to bolster digital defenses. *The Record*. 2023. 10 May. URL: https://therecord.media/latvia-hunt-forward-cyber-command-canada
74. Georgia joins NATO's cyber threat intelligence sharing platform. *Civil Georgia*. Tbilisi. 2020. 6 May. URL: https://civil.ge/archives/341128
75. Cyber incident response capability established in the Republic of Moldova with NATO support. *NATO News*. 2021. 21 January. URL: https://www.nato.int/cps/en/natohq/news_180758.htm

76. Lewis J. A. Cyber War and Ukraine. *Center for Strategic and International Studies*. Washington. 2024. 15 October. URL: https://www.csis.org/analysis/cyber-war-and-ukraine
77. National Strategic Review 2022. *SGDSN* (Secrétariat général de la défense et de la sécurité nationale). Government of France. Paris. 2022. URL: https://www.sgdsn.gouv.fr/files/files/rns-uk-20221202.pdf
78. Paul C., Matthews M. The Russian "firehose of falsehood" propaganda model: Why it might work and options to counter it. *RAND Corporation*. 2016. URL: https://www.rand.org/pubs/perspectives/PE198.html
79. Helmus T.C. et al. Lessons from the information war in Ukraine. *RAND Corporation*. 2024. URL: https://www.rand.org/pubs/research_reports/ RRA2085-2.html
80. Avant D.D. From mercenary to citizen armies: Explaining change in the practice of war. *International Organization*. 2000. Vol. 54, No. 1. P. 41-72.
81. Finland's Cyber Security Strategy 2024–2035. *Prime Minister's Office Finland.* Government Publications. Helsinki. 2024. No. 2024:38. URL: https://julkaisut.valtioneuvosto.fi/handle/10024/165893
82. Schmitt M.N. Ukraine, cyberattacks, and the lessons for international law. *American Journal of International Law*. Cambridge. 2022. Vol. 116, No. 4. P. 654-677. URL: https://www.cambridge.org/core/journals/american-journal-of-international-law/ article/ukraine-cyberattacks-and-the-lessons-for-international-law/69B36016B06998 BCE1EC67C757CDF34D
83. Takács M. The cyber dimension of the Russo-Ukrainian war and its implications for Hungary. *Nemzet és Biztonság*. Budapest. 2024. Vol. 17, No. 1. P. 34-69. URL: https://real.mtak.hu/217708/1/004_M%C3%A1rk%2BTak%C3%A1cs_34-69.pdf
84. National Strategic Review 2025. *SGDSN* (Secrétariat général de la défense et de la sécurité nationale). Government of France. Paris. 2025. URL: https://www.sgdsn.gouv.fr/files/files/Publications/20250713_NP_SGDSN_RNS 2025_EN_0.pdf