Ukraine Foundation

Ukraine as the Cyber Spanish Civil War

By William Dixon
Senior Fellow, Cybersecurity and Technology

In *Ukrainian Policymaker*

June 2025

UKRAINE FOUNDATION
FELLOWSHIP
PUBLICATIONS

Ukraine as the Cyber Spanish Civil War

William Dixon[1]

Associate Fellow, Royal United Services Institute (London, UK),

Senior Tech and Cyber Fellow Ukraine Foundation (Geneva, Switzerland)

E-mail: williamjamesdixon@gmail.com
https://orcid.org/0009-0009-9854-659X

Dixon, William (2025) Ukraine as the Cyber Spanish Civil War. *Ukrainian Policymaker*, Volume 16, ..-... https://doi.org/10.29202/up/16/4.....

The Russo-Ukrainian War, much like the Spanish Civil War, serves as a military laboratory—this time for the integration of cyber capabilities in modern state-on-state conflict. Applying Thomas Rid's triptych of espionage, sabotage, and subversion, this article re-examines Russian and Ukrainian cyber activity from 2022–(June) 2025, drawing exclusively on open-source intelligence[2]*. It finds that cyber espionage has evolved from long-range strategic surveillance to real-time battlefield targeting (e.g., Russia's "Infamous Chisel"); cyber sabotage, while tactically impactful when synchronized with kinetic action, remains strategically limited (e.g., contrasted with Ukraine's "Operation Spiderweb"); and cyber-enabled subversion is pervasive but poorly institutionalized in the West—though Ukraine's authenticity-driven counter-disinformation campaigns demonstrate meaningful impact.*

Crucially, Ukrainian initiatives reveal Kyiv's emergence as an active shaper—not merely a target—of the cyber domain. Through civil-military fusion, private-sector alignment, and crowd-sourced intelligence, Ukraine's model has proven more responsive and integrated than Russia's, despite the latter's deeper technical bench. This comparative analysis underscores that organizational agility—not technical sophistication alone—is the critical determinant of cyber effectiveness. The article concludes by outlining key policy and doctrinal questions NATO allies must address to absorb the strategic lessons of this digital Spanish Civil War.

Keywords: Cyber warfare; Russo-Ukrainian War; Strategic autonomy; Cyber espionage; Cyber sabotage; Cyber subversion; Military innovation; Digital conflict; NATO policy

Received: 08 June 2025 / Accepted: .. June 2025 / Published: .. June 2025

---

[2] Methodology. This analysis employs open-source intelligence (OSINT) methodology, drawing on industry reports, government advisories, and forensic analyses of malware campaigns. The OSINT approach ensures transparency and enables replication of findings. Data spans from 2022 through June 2025, with findings triangulated across technical, geopolitical, and primary sources to mitigate single-source bias. Limitations. Several limitations constrain this analysis. First, reliance on open sources creates inherent gaps, as many cyber operations—particularly successful ones—remain classified due to the sensitive nature of the ongoing conflict. Second, apparent disparities exist between Ukrainian and Russian information disclosure practices regarding cyber operations, potentially introducing systematic bias into available source material. Finally, this analysis examines an active, rapidly evolving conflict where new information continuously emerges, meaning conclusions may require revision as circumstances develop. Despite these constraints, the substantial volume of OSINT on Russo-Ukrainian cyber activity enables meaningful analytical insights, though readers should interpret findings within the context of an ongoing and dynamic situation.

Introduction

The Spanish Civil War (1936–1939) is widely seen by historians as a precursor to the Second World War, not just in ideology or geopolitics, but in military innovation. An arena where emerging doctrines, weapons systems, and international alignments were tested by proxy (Mumford, 2013). It served as a live-fire laboratory for what were then frontier technologies: German dive-bombers, Soviet armor, and combined arms tactics.

As scholars of military innovation have demonstrated, conflicts often serve as crucial laboratories for emerging technologies and doctrines, with innovations diffusing rapidly across military organizations when their battlefield utility becomes apparent (Rosen, 1991; Horowitz, 2010; Posen, 1984). This dynamic has been particularly evident during periods of military transformation, where new technologies challenge existing doctrines and organizational structures (Sapolsky et al., 2009). Today, the war in Ukraine plays a similar role. It is both a crucible for new weaponry and doctrine, and the first protracted test of cyber capabilities in a state-on-state conflict (Black et al., 2024). Like Spain in the 1930s, Ukraine warns of what is to come—if we choose to listen.

Before the Russian invasion, many commentators anticipated that this would "redefine cyber warfare" (Politico, 2022). As widely reported in U.S. media and commentary in the run-up to the invasion (Iyengar, 2022; Remnick, 2022; Gunderman, 2022; Time, 2022), many anticipated major digital disruption, and paralyzed infrastructure—delivered by what was assessed to be a true tier-one cyber power. But this conflict did not unfold as many predicted (Black et. al., 2024) with some even asking simply – "Where is Russia's cyber blitzkrieg?" (The Hill, 2022).

This reflected a broader scholarly debate stretching back over two decades about whether cyber operations constituted a transformative new domain of warfare (Arquila & Ronfeldt 1993, Libicki, 2007; Rid, 2011; Kello, 2013). Skeptics like Valeriano and Maness have consistently argued that cyber conflict's effects are often overstated, with most operations falling short of their predicted strategic impact (Valeriano & Maness, 2015).

Contemporary scholarship has further refined this debate, with Borghard and Lonergan (2017) developing a logic of coercion in cyberspace, while Lindsay (2013) has demonstrated the operational constraints that limit cyber warfare's strategic utility. Similarly, Gartzke and Lindsay's work on cyber power theory suggests that digital capabilities may be more constrained by political and strategic factors than pure technical potential (Gartzke & Lindsay, 2017).

The Ukrainian experience provides crucial empirical evidence for evaluating these competing theoretical frameworks – with this article fitting squarely within a corrective tradition in cyber studies that seeks to challenge both the "cyber revolution" thesis and the "cyber irrelevance" position.

1. "Cyber War" As Is. Not Imagined

The dramatic “lights-out” scenarios forecast by analysts and media outlets failed to materialize. Instead of a momentous first-strike cyber blitzkrieg, the conflict has featured a long, grinding, and adaptive use of cyber capabilities (Davydiuk & Potii, 2024). They have progressively become more effective and integrated over the duration of the conflict (Black, 2024) and are better understood as a series of related activities which can cumulate in strategic impact as opposed to single decisive events.

This was not the first time that the domain has been prone to hyperbolic predictions (Rid, 2011). A cyber generation before, Thomas Rid argued in 2011’s *Cyber War Will Not Take Place* that, contrary to sensationalist forecasts of impending digital “Pearl Harbours”, that cyber operations did not constitute acts of war in the traditional, Clausewitzian sense. Instead, cyber was “non-violent” and fell into three empirically grounded categories: espionage (clandestine intelligence), sabotage (disruption), and subversion (deception).

Applying Rid’s framework—which has become foundational in cyber conflict literature and been extensively built upon by scholars such as Buchanan (2020), Sanger (2018), and others studying digital conflict—now to the Ukrainian context allows us to move beyond myths and grasp the tactical and strategic realities of cyber conflict both now and in the future. This isn’t cyber war as imagined nor ignored—it is cyber war as *it actually exists*: increasingly embedded in military campaigns, able to support or augment kinetic operations, and evolving with both battlefield and strategic needs rather than supplanting them.

2. Russian Doctrine. Anticipation Meets Reality

2.1. Espionage: From Strategic Intelligence to Tactical Cyber ISR?

Espionage remains the most established function of cyber power. Yet in Ukraine, it has evolved from slow, strategic surveillance into a tactical battlefield enabler—reshaping how militaries think about targeting and tempo.

Strategic espionage has been the most persistent form of cyber activity in Ukraine since the earliest days of Russian aggression. State-linked groups associated with the FSB, SVR and GRU, such as APT28 Fancy Bear, Sandworm, and Gamaredon, have successfully targeted Ukrainian political, military, and economic targets to inform planning and high-level decision making with great effect (Mandiant, 2023; CyberScoop, 2025; U.S. DoD, 2025; Politico, 2023). Arguably though, this type of activity was a natural extension of long-term cyber intelligence gathering Russian APTs had become known for in the previous decade. While important, not necessarily—*new*.

What is new—and historically significant—is the tactical deployment of cyber espionage in direct support of battlefield operations (Black, 2024), effectively expanding Rid’s category of espionage beyond strategic intelligence-gathering into real-time cyber-ISR and kinetic, violent effects. A doctrinal shift; just as the Spanish Civil War marked air power's shift from mere reconnaissance to operational bombing, research by CrowdStrike, Google Mandiant, and others has revealed that

the same Russian APTs traditionally focused on strategic cyber intelligence gathering have bridged this critical step (Coker, 2024).

The most high-profile example so far has been the GRU developing and deploying the *Infamous Chisel* malware to penetrate and track Android devices at scale used by Ukrainian military personnel. This enabled them to identify front-line troop movements in near real time and allowed Russian battlefield operators to precisely locate units and subsequently direct artillery or drone strikes (NCSC et al., 2023). This evolution aligns with Maschmeyer's (2021) work on cyber persistence theory, which emphasizes how sustained access enables real-time operational support rather than merely strategic intelligence collection. As Smeets (2018) argues, offensive cyber operations achieve strategic value primarily through their integration with broader military campaigns rather than as standalone instruments.

Tactical Cyber-ISR blurs the lines between cyber, SIGINT, and electronic warfare (RAND Corporation, 2024). With the right conditions and interoperability, malware can directly support battlefield decision-making in real time (NCSC et al., 2023), challenging Western assumptions that cyber operations are solely strategic tools. Yet Russia's institutional architecture stifles this cyber potential. As Giles (2023), Sherman (2025) and others indicate, Russian Agencies often operate as competing fiefdoms, with a primary focus on strategic intelligence and subversion (Melella et al., 2024)—each hoarding capabilities and resisting integration with conventional forces. This fragmentation has potentially created critical bottlenecks: tactical cyber intelligence often stalling, with operators struggling to share data with battlefield commanders (Melella et al., 2024; Giles, 2023). Analysts attribute this not just to rigid hierarchies (Melella et al., 2024), but to a deeper pathology: Putin's system incentivizes parallel structures to prevent any single agency from becoming too powerful. The result is a technically sophisticated but potentially bureaucratically crippled cyber force, unable to fully exploit perishable intelligence.

2.2. Cyber Sabotage: Disruption, Not Destruction

If espionage shows cyber's potential to compress decision cycles, sabotage tests its ability to create decisive disruption. Cyber sabotage is often imagined as a substitute for kinetic force—a digital way to disable infrastructure or paralyse an enemy. The war in Ukraine reveals both tactical utility, but enduring limitations of this function.

Ukraine has long been a proving ground for Russian cyber sabotage. The 2015–2017 grid attacks and the NotPetya malware campaign marked a high watermark of destructive capability (Greenberg, 2018; Giles, 2017). Since the full-scale invasion in 2022, however, Russia's cyber sabotage has shifted toward more episodic, synchronized, and psychologically disruptive campaigns, focused on battlefield friction and infrastructure denial. This aligns with Wilde's (2024) observation that Russia's cyber sabotage is increasingly psychologically calibrated to *amplify* the effects of the wider kinetic war rather than replace them—a doctrinal adaptation to Ukraine's resilience.

Initial wartime operations included wiper malware such as WhisperGate and HermeticWiper, which aimed to degrade Ukrainian institutional resilience and delay mobilization (CISA, 2022). These attacks were strategically timed to coincide with kinetic strikes and the initial troop movements, integrated into Russia's overarching "Shock and Awe" doctrine. Russian operators also attempted to disable satellite communications via Viasat (Schulze, 2024) and executed numerous campaigns against critical infrastructure systems (Giles, 2023).

After this initial period and the stalling of the main campaign, cyber campaigns have been detected that sought to disrupt transport logistics or erase battlefield communications, often coinciding with kinetic manoeuvres (Google Cloud, 2024). Ukrainian CNI providers have been compromised, potentially for cyber sabotage, by the APT Sandworm and were exposed in 2025 (ESET, 2025). Sabotage efforts (and espionage) have often been identified, mitigated, or contained through improved Ukrainian cyber defences and an unprecedented fusion of military, government, and private-sector capabilities, including CERT-UA, Microsoft, security companies, and Western intelligence services (Microsoft, 2022, 2025; NSA, 2025; Smith, 2022). This experience underscores a new operational reality: effective cyber resilience requires a fully interoperable and integrated civil-military-industrial architecture (Wilner et al., 2024).

In practice, cyber sabotage still struggles to match the scale and persistence of kinetic effects, especially when contrasted with Ukraine's other sabotage operations. Operation Spider's Web was a meticulously planned drone assault, targeting strategic airbases deep inside Russia. Over 18 months, Ukraine's Security Service (SBU) covertly transported explosive-laden drones into position. It ultimately caused an estimated $7 billion in damages and incapacitated over a third of Russia's strategic bomber fleet (BBC, 2025; Bondar, 2025). It starkly contrasts the tangible, immediate impact of kinetic sabotage with the transient effects of cyber. Digital-enabled sabotage is both real and evolving—but not magical.

Critically, Russia's doctrinal emphasis on first-strike, high-visibility disruption may have limited its flexibility in prolonged campaigns. Analysts suggest that Russia expected to frontload cyber operations for maximum early psychological shock and logistical paralysis—a strategy ill-suited for the adaptive, attritional character of the war (Giles, 2023; SWP, 2023). Moreover, limited private-sector integration and siloed command structures have impeded real-time operational feedback, reducing the learning curve for Russian cyber planners and contributing to stagnation in capability deployment (Melella et al., 2024; CEPA, 2023).

2.3. Cyber Subversion: Digital Disinformation at Scale

Subversion is where cyber power most diverges from conventional warfare. Unlike espionage or sabotage, subversion targets perception, not infrastructure. Its tools are leaks, bots, and influence networks—not necessarily malware. Russia has long excelled in this domain, but Ukraine's counter-disinformation efforts reveal how narrative control and credibility can become powerful asymmetric tools in their own right.

Of the three domains, cyber subversion is where Russia has achieved its most consistent and enduring effects. Long-practiced information warfare has been adapted to the digital age, shaping both battlefield morale and international perception (CEPA, 2023; Melella et al., 2024). It is also the one cyber domain where Moscow can draw on a wide swathe of cross-society actors, from state agencies to proxy influencers (Schnurr, 2025). Frontline soldiers are a frequent target of adversary campaigns to undermine the will to fight and unit cohesion. at the start of the war were used to sow confusion and disrupt troops cohesion (Helman & Holynska 2024), while coordinated online disinformation campaigns have coincided with wavering legislative support in key NATO states. Cyber subversion has become a core pillar of Russia's modern way of war, enabled by the integration of offensive information operations within centralized military-intelligence command structures (Melella et al., 2024). Yet it remains the most inconsistently countered part of the cyber spectrum by both Ukraine and the West (Bennhold, 2025), due in part to its ambiguous status between warfare, intelligence, and communication.

Strategically, Moscow's "firehose of falsehood" approach has targeted Western audiences with influence operations designed to erode support for Ukraine (Paul & Matthews, 2016). Officials in Germany and the United States have noted surges in online misinformation preceding critical parliamentary debates on arms packages. Platforms such as Meta and X (formerly Twitter) have removed thousands of fake, Russian-linked accounts; one operation documented by Meta in 2022 alone dismantled over 1,600 coordinated profiles spreading false narratives in Polish, German, Italian, French, and English (Meta, 2022).

Tactically, Russia has developed "micro-targeting" of Ukrainian frontline units and communities including during the 2024 assault on Kharkiv where there was a deeply integrated sustained subversion campaign working in-lock step with kinetic attacks and military decision making (Hunder, 2024). According to reports from Ukraine's Centre for Strategic Communication and Information Security (CSCIS), along with broader analyses of Russian hybrid warfare tactics, such messaging is a frequent occurrence—prompting battlefield commanders to incorporate counter-disinformation protocols into real-time decision-making (Giles, 2023). Yet Russia's cyber subversion apparatus is not without limitations. At times, the lack of integration with civil society or the domestic tech sector has hindered its adaptability and unlike Ukraine's diaspora-led digital activists, Russia largely lacks a bottom-up informational ecosystem, potentially a reflection of the rigidity of Putin's centralization of power—a systemic constraint that stifles the bottom-up innovation seen in Ukraine's IT Army.

Despite its centrality to modern hybrid warfare, cyber-enabled subversion remains one of the least institutionalised and most ambiguously governed aspects of national cyber strategy. Multiple NATO and Western policy reviews have highlighted the lack of coherent doctrine, institutional ownership, and dedicated operational capacity for countering foreign digital influence operations (NATO StratCom COE, 2023; U.S. Senate Intelligence Committee, 2019). It is unclear who owns the problem—divided among military psychological operations units, intelligence services, civilian ministries, and private-sector platforms—with limited cross-agency coordination (Pamment, 2022; Wanless & Berk, 2021). This fragmentation impairs timely response and long-term strategic resilience. Unless subversion is addressed

with the same doctrinal clarity and institutional investment as espionage or critical infrastructure defence, it will remain an enduring structural weakness—an unpatched vector in the West's otherwise maturing cyber posture (Rid, 2020).

3. Ukrainian Initiative.

From Cyber Target to Cyber Power

To draw comparative lessons from Rid's triptych (see also Figure 1), we assess how Russia and Ukraine performed across each function—espionage, sabotage, and subversion—highlighting divergence in effectiveness and adaptability.

Ukraine has been in cyber discourse primarily viewed as a victim—Europe's 'petri-dish' for Russian digital aggression (Sanger, 2018). But since 2022, Kyiv has demonstrated that it is not merely enduring cyber conflict—it is actively shaping it. Their efforts have delivered with speed and scale, outpacing the capabilities of more formally resourced counterparts and critically often outmatched their Russian counterparts.

Ukraine has demonstrated that it can innovate rapidly across all three of Rid's domains—espionage, sabotage, and subversion—often matching or out-performing Russia despite far smaller resources. Three factors explain this shift: deep private-sector partnerships, the mobilisation of civil-society volunteers, and a flexible doctrine that blends state authority with decentralised initiative. The crowd-sourced IT Army of Ukraine, in particular, has matured from ad-hoc hacktivism into a semi-coordinated auxiliary (Kirichenko, 2025). These volunteer efforts are not by accident; instead, they are a manifestation of the legal and strategic foundation laid by the National Cybersecurity Strategy and implementations made at the onset of the war by the Ministry of Defence (Schectman & Bing, 2022; Renden-Katolik 2023). Volunteer capacity now extends state objectives at minimal fiscal cost; Universities, private cyber-firms, and diaspora networks further widen the talent pool, turning societal mobilisation into a strategic asset Russia has struggled to match.

This organizational configuration reflects what scholars identify as "networked governance" (Goldsmith & Eggers, 2004) and "collaborative advantage" (Huxham & Vangen, 2005)—models where distributed coordination across organizational boundaries can generate capabilities exceeding the sum of individual parts. Drawing on Allison and Zelikow's (1999) organizational behavior models, Ukraine's approach demonstrates how institutional flexibility can overcome traditional bureaucratic constraints, while Russia's centralized structure exhibits classic symptoms of organizational inertia that limit adaptive capacity (Avant, 1994).

3.1. Espionage: A Fledgling APT?

Kyiv now operates a two-tier intelligence (state and non-state) model able to establish strategic intelligence-gathering capability as well as the ability to integrate into battlefield operations. At the state level, Ukraine appears capable of APT-level strategic intelligence gathering, as has been publicly disclosed in operations against the Tupolev Aerospace Design Bureau (News.com.au, 2024), the Russian Defence Ministry (Kyiv Independent, 2024), and a high-value Russian electronic military

document system (GUR, 2024). From a battlefield perspective—while nothing publicly compares to the disclosure of Infamous Chisel—state-led tactical cyber intelligence has been innovative, reportedly including the use of drone technology (Forbes, 2025) and instances of using data from apps with fake profiles to extract information on enemy troop movements for kinetic targeting (CNN, 2024).

Similarly, volunteer groups such as Cyber Resistance and the Cyber Community for Free Ukraine scrape Russian social media, flight-tracking feeds, and publicly exposed sensors; their findings can move from collection to fires tasking in under two hours, contrasting with Russia's more centralised, slower decision process (The Times, 2024). The chief limitation remains processing capacity: analysts must be selective to avoid saturating bandwidth and attention—an economy Moscow's larger SIGINT bureaucracy rarely faces (Melella et al., 2024; CEPA, 2023). Despite these advancements, Ukraine's APT activity is likely still much less strategically capable and extensive than Russia's long-established and heavily resourced state operations (CrowdStrike, 2025; CEPA, 2023).

3.2. Sabotage: Tactical Disruptor

Ukraine's two-tier model has also been able to develop and deploy cyber sabotage capabilities. Time-bound tactical and symbolic utility has been derived from such operations—especially when integrated into broader efforts albeit the standalone strategic value remains questionable. In early 2024, Ukraine's military intelligence agency (HUR) hackers reportedly targeted Russian military software used to modify commercial DJI drones for military applications, effectively grounding several drone fleets (Kyiv Post, 2024a; UNN, 2024). Throughout the spring and summer of 2024, a spate of additional attacks included Ukrainian cyber operatives disrupting Moscow's sewer infrastructure (Kyiv Post, 2024b) and targeting airport systems, resulting in widespread disruption (Kyiv Post, 2024c).

Similarly, we also see in this domain sophisticated integrated state and civil cooperation. HUR reported that volunteer BO Team hackers collaborated with them to target servers and data from the Russian state space hydrometeorology research center (Antoniuk, 2025). The IT Army of Ukraine's actions have included distributed-denial-of-service campaigns against targets like TASS, and even the "largest Distributed Denial of Service (DDoS) attack in history" against Russian banks in June 2024 (Cyber Express, 2024). Civil hacktivism has also been shown to become an auxiliary to military efforts when coordinated, including attacks against Russian CCTV networks to disrupt surveillance during drone strikes on oil refineries—a potentially important development (Kirichenko, 2025 This civil hacktivism aligns to Dunn Cavelty and Wegner's (2022) observations on cyber's inherent security pluralism and shifting governance, with Ukraine's two-tier model delivering decentralized innovation with overall state oversight.

3.3. Subversion: Authenticity and Counter-Disinformation

While often reported—rightly—as a victim of Russian information warfare (Linvil & Warren, 2025), Ukraine's two-tier model has developed a growing proficiency in digital influence—even as counter-disinformation remains its principal focus. Rather than rely on saturation, Kyiv emphasizes strategic authenticity:

leveraging verified content, targeted messaging, and rapid media amplification (Danchenkova, 2025). This approach was evident during the 2022 Kherson offensive feint (Harding, 2022) and again in Operation Spiderweb (Robertson, 2025), where battlefield actions were reinforced through carefully orchestrated information releases. Ukrainian forces have also used platforms like Telegram to disseminate morale-targeted messages, including graphic combat footage aimed at degrading Russian cohesion (Browne, 2024).

Given the scale of Moscow's information efforts, Ukraine's innovation lies in how it has countered Russian disinformation. Its approach combines centralized coordination with decentralized execution—leveraging civil society, tech partnerships, and narrative credibility to outpace adversaries (Danchenkova, 2025). State efforts, such as the 2022 media law expanding regulatory powers (Council of Europe, 2025), are blended with other efforts such as joint actions with the Centre for Countering Disinformation (RNBO, 2025). Volunteers have even engaged in memetic counter-information warfare via Twitter, producing culturally resonant content to highlight Russian failures and erode troop confidence (Oosterveld et al., 2023). Much more research is needed to understand how Ukraine's adaptive strategic communications model—including its effectiveness—can inform broader NATO and EU counter-disinformation efforts.

Taking all three domains together, state-led intelligence intrusions, targeted and disparate sabotage, credibility-driven subversion, and broad volunteer participation have transformed Ukraine into a genuine architect of contemporary cyber doctrine. While the model is shaped by existential threat and exceptional foreign assistance—and therefore not directly transferable to all allies—it illustrates how agility, openness, and public-private integration enable a mid-sized democracy to contest a nominal cyber super-power on near-equal terms. The ecosystem is strong today, but its long-term sustainability still depends on continued Western technical and intelligence support, political alignment and corporate policies, none of which are guaranteed or static.

Table 1: Rid's Triptych: Russia vs. Ukraine in Cyber Conflict (2022–June 2025)

Domain	Russia	Ukraine
Espionage	Persistent access via advanced implants; developed tactical ISR capability; potentially bottlenecked by stovepiped military-cyber coordination.	Agile, two-tier intelligence model; rapid OSINT-to-fires loop; less technically advanced but faster and more integrated.

Sabotage	High-impact wipers; front-loaded doctrine aimed at early shock; limited adaptability in sustained campaigns.	Precision, low-attribution ops; civil-military coordination; resilience-focused defense posture.
Subversion	Volume-driven disinformation at scale; targets Western cohesion and frontline morale; weak integration with civil society.	Credibility-driven info ops; uses authentic leaks and OSINT; coordinated narrative strategy with diaspora and volunteers.

4. Strategic Balance Sheet: What the Russo-Ukrainian War Really Tells Us About Cyber

First, the war confirms what many policy makers already know—cyber espionage continues to be a premier instrument for strategic intelligence gathering. However, both Moscow's Infamous Chisel and Kyiv's own innovations show that well-placed cyber intelligence can deliver frontline coordinates or logistics manifests faster and more cheaply than satellites or manned reconnaissance (Maschmeyer, 2021; Lindsay, 2013). At a tactical level the available case studies still show a dependency on complementary data and targeting chains: cyber intelligence might locate an artillery battery, but ballistic corrections still rely on drones, counter-battery radar, or HUMINT. It still remains to be seen if cyber can ever truly provide the level of visibility, reliability and assurance to fully supplant traditional collection methods at this level as a standalone capability, recognising though it can augment operations.

Second, the conflict exposes the ceiling on cyber sabotage as a substitute for kinetic attack. Precision wipers can delay fuel convoys or paralyse databases, but their effects are temporary and often reversible within days. In contrast, Ukraine's kinetic Spider's Web drone offensive disabled a third of Russia's strategic bomber fleet for months and imposed multi-billion-dollar losses. The lesson is that digital disruption is most effective when synchronised with physical force or diplomacy—not when asked to carry the strategic burden alone (Borghard & Lonergan, 2017). Standalone cyber sabotage may remain uniquely suited to deniable, non-violent, disruption below the threshold of war, a feature especially valuable in constrained diplomatic theatres—the most famous of which, still remains the Stuxnet Case study.

Third, cyber's greatest asymmetric promise lies in the subversion domain, where information operations blend speed, deniability, and global reach. Russian "fire-hose" propaganda achieves volume and is a domain where Moscow can demonstrate levels of cyber interoperability to erode enemy morale and shape allied legislation. Subversion indicates cyber's strategic ambivalence: the same tools that empower democratic resilience can bolster authoritarian disinformation. Cyber, then, is neither a silver bullet nor a busted flush—it is a force multiplier whose impact depends on integration with kinetic assets, narrative authority, and the resilience of the societies that wield it.

Fourth, improvements in cyber effectiveness during the war have stemmed less from technical breakthroughs and more from organisational innovation and interoperability (Cote, 2000; Horowitz, 2010). Ukraine's ability to coordinate between state agencies, allied partners, private-sector providers, and civilian volunteers has delivered faster adaptation and richer situational awareness than any single technological leap. By contrast, Russia's more centralised and hierarchical model has arguably struggled to keep pace with the distributed innovation of its adversary (Allison & Zelikow, 1999).

Ukraine's most underappreciated advantage may be its ability to orchestrate a horizontally integrated cyber ecosystem—fusing inputs from foreign state partners, private-sector providers, and decentralised civil society actors. From Palantir's analytics (United24 Media, 2024) and Microsoft's telemetry to diaspora-led digital forensics and grassroots OSINT collectives, this pluralistic architecture enables agility and reach that a more centralised, vertically controlled system like Russia's struggles to replicate. Cyber effectiveness depends less on raw technical power than on leadership, integration, and agile partnerships capable of thinking laterally and adapting in real time.

5. Future Research Questions

The Russo-Ukrainian War reveals that cyber effectiveness depends less on technical capability alone and more on organizational agility, strategic communication, and civil-military integration. Ukraine's decentralized and adaptive approach contrasts sharply with Russia's rigid and centralized model—reflecting broader lessons from military innovation literature, where doctrine and structure often outweigh raw capacity (Cote, 2000). Building on these insights, three critical research questions emerge:

- How do Russia's institutional characteristics—centralized command structures, limited private-sector integration, and rigid doctrinal assumptions—impede its operational agility in the cyber domain, and what does this reveal about the broader challenges authoritarian systems face in adapting to dynamic, protracted cyber conflict?

- What does Ukraine's strategic communications model reveal about effective approaches to countering cyber-enabled disinformation, and which of its practices—such as decentralized execution, authenticity-based messaging, and civil society integration—can be adapted by other democracies to enhance their cognitive resilience?

- How do different organizational models (Liebetrau, 2022)—centralized vs. networked, state-led vs. public-private—shape cyber operational effectiveness in protracted conflict, and what lessons can be drawn from Ukraine's hybrid approach to inform future doctrine and force design in NATO countries?

Answering these questions is crucial for understanding not only the mechanisms behind Russia's cyber operational performance, but for informing Western strategic planning against similar adversaries.

6. From Madrid to Mariupol—Strategic Implications for Policy Makers

While the previous section outlined some core research questions, this final section considers the immediate strategic imperatives for policymakers across NATO and allied institutions. Building on Ukraine's example, NATO states must address capability, doctrinal, and measurement challenges to future-proof their cyber posture.

The Spanish Civil War foreshadowed the tactics and technologies of global conflict, now, Ukraine's war is quietly rewriting our understanding of cyber's role in modern warfare. Yet the picture is uneven. Cyber operations have become more integrated across military levels—but their effectiveness across Rid's three domains varies significantly. Espionage is becoming tactically relevant, sabotage remains constrained, and subversion is widespread but poorly understood or countered. For Ukraine's allies, the most important question is not whether cyber war is happening —but whether their own institutions are prepared to meet its challenges. To that end, three questions must now be urgently addressed:

1. What are the most critical capability gaps exposed by Ukraine's experience? National cyber commands, military planners, and defence ministries across NATO and allied states must now conduct clear-eyed assessments of where their own doctrines, force structures, and partnerships fall short—highlighted by Ukraine's fusion of, and focus on, civil, corporate, and classified cyber capabilities as a unified whole.

2. How should strategic priorities shift now that cyber has proven to be neither a war-winning silver bullet nor an irrelevant sideshow, but a complex, evolving instrument of modern warfare? Senior decision-makers in defence ministries, intelligence agencies, and legislative oversight bodies must recalibrate expectations and budgets to reflect cyber's true, demonstrated utility—not its imagined potential—a shift Ukraine made by treating cyber as a supporting arm, not a standalone domain.

3. What research and policy frameworks are needed to empirically track cyber's operational effectiveness across conflict types—moving beyond threat inflation and towards grounded strategic planning? Here, responsibility falls to national security think tanks, academic institutions, and government-affiliated research bodies to establish the methodologies and datasets that can reliably inform future planning. Ukraine's experience highlights the need to measure cyber impact over time and across tactical, operational, and strategic levels—not just by headline-grabbing attacks.

The Western alliance must now rapidly absorb and apply the lessons of this conflict, including those drawn from Ukraine's cyber defensive and offensive innovations. We must move beyond headline-driven assessments and ground our understanding in empirical evidence—lest we repeat the complacency seen after Guernica, when observers failed to act on the warning. That is a lapse modern adversaries are counting on.

The Spanish Civil War analogy proves instructive beyond mere historical parallel, reflecting broader patterns of proxy conflict where great powers test capabilities and doctrines through surrogate engagements (Mumford, 2013). Just as

observers in 1939 who understood the tactical innovations of combined arms warfare, strategic bombing, and mechanized operations gained decisive advantages in the subsequent global conflict, nations that internalize Ukraine's cyber lessons may find themselves better prepared for future digital-physical warfare.

The analogy also warns against over-generalization: Spain's lessons were most applicable to European continental warfare, less so to Pacific island campaigns or desert operations. Similarly, Ukraine's cyber innovations may prove most relevant to conflicts involving peer competitors with comparable technological infrastructure and democratic governance structures.

The window for learning from Ukraine's cyber laboratory is finite. As the conflict evolves and participants adapt, early lessons may become obsolete or deliberately obscured by operational security requirements. Doctrinal recalibration must tread carefully. Ukraine's cyber integration, forged under existential threat and exceptional partnerships, may not be directly replicable across NATO. Still, its core principles—speed, openness, and integration—offer critical lessons. Adversaries are closely observing the cyber lessons emerging from Ukraine.

Above all, allies must hard-wire cognitive security—digital literacy, civic OSINT, and rapid debunking—as an operational imperative, or risk losing future conflicts in browsers before it gets to the battlefield. We cannot afford to lag behind. The time for theoretical debates about cyber war's potential has passed; the imperative now is preparation for cyber as it actually exists.

7. Conclusion—Redefining Cyber Conflict

The Russo-Ukrainian War has fundamentally altered how we understand cyber conflict, not least by extending Rid's original conceptual framework through tactical cyber-ISR's operationalization of espionage and Ukraine's weaponization of authentic subversion—evolutions that demand doctrinal reassessment. This analysis reveals cyber operations as neither the decisive "silver bullet" nor irrelevant sideshow that analysts predicted, but as an increasingly integrated component of military operations whose effectiveness varies dramatically across domains and organizational contexts.

It is clear that cyber has evolved, moving from broader strategic intelligence to direct tactical battlefield support, as evidenced by Russia's Infamous Chisel campaign, which highlighted malware's capability to deliver actionable targeting data in near real-time. Cyber sabotage, while tactically valuable, still faces strategic limitations, unable to achieve the sustained physical effects of kinetic alternatives like Ukraine's Spider's Web drone offensive. Furthermore, cyber subversion stands out as the domain's most significant asymmetric promise, showcasing how Ukraine's authenticity-driven information operations effectively compete against Russia's volume-based disinformation, influencing both battlefield morale and allied legislative support. Ukraine's transformation into an active cyber power also shows that organizational agility, civil-military fusion, and horizontal integration matter more than size or scale. These traits allowed a mid-sized democracy to challenge a cyber superpower.

This analysis contributes to cyber conflict scholarship in several ways. Empirically, it provides a comprehensive application of Rid's triptych to a protracted state-on-state conflict, revealing how each domain performs under sustained operational pressure rather than isolated incidents. The findings challenge prevailing assumptions about cyber escalation and effectiveness, particularly the notion that advanced persistent threat capabilities automatically translate into battlefield advantage (Gartzke & Lindsay, 2017; Kello, 2013). It ultimately provides empirical evidence for the "corrective tradition" and identifies new pathways to cyber effectiveness.

Theoretically, the analysis also highlights the crucial role of organizational factors in cyber effectiveness—a dimension often overlooked in technically-focused scholarship. As alliance burden-sharing theories suggest, Ukraine's ability to leverage Western technical support while maintaining operational autonomy demonstrates new models of collaborative warfare that may characterize future conflicts (Olson & Zeckhauser, 1966).

Ukraine's resilience stems not from superior malware or novel attack vectors, but from its ability to orchestrate diverse stakeholders across government, private sector, and civil society into a coherent cyber ecosystem while retaining leadership. This experience underscores the importance of institutional design, not just technical capacity, in shaping cyber outcomes. As the domain continues to evolve, future research must pay closer attention to these structural enablers of effectiveness—and policymakers must recognize that strategic advantage in cyberspace may hinge as much on integration and agility as on tools and talent.

⍰ References

Allison, G. T., and Zelikow, P. (1999) Essence of Decision: Explaining the Cuban Cyber Crisis (2nd ed.). New York: Longman.

Antoniuk, D. (2025) Pro-Ukraine hacker group Black Owl continues to pose a major threat to Russia. *The Record*. Available online: https://therecord.media/pro-ukraine-hacker-group-black-owl-major-threat-russia

Arquilla, J., and Ronfeldt, D. (1993) Cyberwar is Coming! RAND Corporation, Available online: https://www.rand.org/pubs/reprints/RP223.html

Avant, D. D. (1994) Political Institutions and Military Change: Lessons from Peripheral Wars. Ithaca: Cornell University Press.

BBC (2025) How Ukraine carried out a daring 'Spider Web' attack on Russian bombers. June 1. Available online: https://www.bbc.com/news/articles/cq69qnvj6nlo

Bennhold, K. (2025) Britain Confronts Cyber Threats from Russia and Iran as Election Nears. *The New York Times*. June 6. Available online: https://www.nytimes.com/2025/06/06/world/europe/uk-russia-iran-state-threats.html

Black, D. (2024) Russia's cyber campaign shifts to Ukraine's frontlines. Royal United Services Institute. July 21. Available online: https://www.rusi.org/explore-our-research/publications/commentary/russias-cyber-campaign-shifts-ukraines-frontlines

Black, J., Paillé, P., Kleberg, C., Ellis, C., and Sommerfeld Antoniou, M. (2024) Russia's War in Ukraine: Emerging Insights for UK and NATO Joint Doctrine. RAND Corporation.

Blessing, J. (2022) Where is Russia's cyber blitzkrieg? *The Hill*. March 9. Available online: https://thehill.com/opinion/cybersecurity/597272-where-is-russias-cyber-blitzkrieg/

Bondar, K. (2025) How Ukraine's Operation "Spider's Web" Redefines Asymmetric Warfare. *CSIS*. June 2. Available online: https://www.csis.org/analysis/how-ukraines-spider-web-operation-redefines-asymmetric-warfare

Bonomo, E. (2022) U.S. Companies Should Prepare for Putin's 'Gangster Diplomacy' As Risk of Russian Cyberattacks Grows. *Time*. February 26. Available online: https://time.com/6151730/chris-krebs-russia-cyberattacks/

Borghard, E. D., and Lonergan, S. W. (2017) The logic of coercion in cyberspace. *Security Studies*, 26(3): 452– 481. Available online: https://www.researchgate.net/publication/316804106_The_Logic_of_Coercion_in_Cyberspace

Browne, D. (2024) Drone chief fights psychological war with videos of dying Russians. *The Times.* May 18. Available online: https://www.thetimes.com/world/russia-ukraine-war/article/drone-chief-fights-psychological-war-with-videos-of-dying-russians-jvvlh0cvr

Buchanan, B. (2020) The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations. New York: Oxford University Press.

CEPA (2023) Russian Cyberwarfare: Unpacking Kremlin Capabilities. Center for European Policy Analysis.

CERT-UA (2024) CERT-UA detects new wave of cyberattacks on Ukraine's defense enterprises. https://cip.gov.ua/en/news/cert-ua-viyavila-novu-khvilyu-atak-na-oboronni-pidpriyemstva-ta-sili-oboroni-ukrayini

Center for Humane Technology (2022) The Invisible Cyber War [Podcast episode]. Available online: https://www.humanetech.com/podcast/55-the-invisible-cyber-war

CISA (2022) Understanding and mitigating Russian state-sponsored cyber threats to U.S. critical infrastructure (Advisory AA22-057A). Cybersecurity and Infrastructure Security Agency. February 26. Available online: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-011a

CNN (2024) Russia uses dating apps near the Ukrainian border. August 21. Available online: https://edition.cnn.com/2024/08/21/world/russia-dating-apps-border-intl

Coker, J. (2024) Russia shifts cyber focus to battlefield intelligence in Ukraine. *Infosecurity Magazine*. July 23. Available online: https://www.infosecurity-magazine.com/news/russia-cyber-focus-battlefield/

Cote, O. R. (2000) The politics of innovative military doctrine: The U.S. Navy and fleet ballistic missiles. *Security Studies*, 9(3): 50–89. Available online: https://dspace.mit.edu/handle/1721.1/11217

Council of Europe (2025) Ukrainian media authorities join pan-European dialogue on countering disinformation. Kyiv Office. Available online: https://www.coe.int/en/web/kyiv/-/ukrainian-media-authorities-join-pan-european-dialogue-on-countering-disinformation

CrowdStrike (2022) CrowdStrike 2022 Global Threat Report. Available online: https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2022GTR.pdf

CrowdStrike (2023) CrowdStrike 2023 Global Threat Report. Available online: https://www.crowdstrike.com/en-us/resources/reports/crowdstrike-2023-global-threat-report/

CrowdStrike (2024) CrowdStrike 2024 Global Threat Report. Available online: https://www.crowdstrike.com/en-us/resources/reports/crowdstrike-2024-global-threat-report/

CrowdStrike (2025) CrowdStrike 2025 Global Threat Report. Available online: https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrikeGlobalThreatReport2025.pdf?version=0

Cyber Express (2024) Russia's VTB Bank Faces Largest DDoS Attack in History. Available online: https://thecyberexpress.com/russia-vtb-bank-largest-ddos-attack/

CyberScoop (2025) LaundryBear and VoidBlizzard among Russian APTs expanding espionage. March 18. Available online: https://cyberscoop.com/laundry-bear-void-blizzard-russia-apt/

Danchenkova, O. (2025) Ukraine's Hard-Won Approach to Strategic Communications and Counter-Disinformation: Lessons for Europe and Beyond. *Tech Policy Press*. March 12. Available online: https://www.techpolicy.press/ukraines-hardwon-approach-to-strategic-communications-and-counterdisinformation-lessons-for-europe-and-beyond/

Davydiuk, A., and Potii, O. (2024) National Cybersecurity Governance: Ukraine. NATO Cooperative Cyber Defence Centre of Excellence. Available online: https://ccdcoe.org/uploads/2024/08/National-Cybersecurity-Governance_Ukraine_Davydiuk_Potii_2024.pdf

DISA (n.d.) Strategic Communication and Counter-Disinformation: Lessons from Ukraine's Experience. Available online: https://disa.org/strategic-communication-and-counter-disinformation-lessons-from-ukraines-experience/

Dunn Cavelty, M., and Wegner, A. (2022), Cyber Security Politics, Socio-Technological Transformations and Political Fragmentation, Routledge. Available online: https://library.oapen.org/bitstream/id/20a53302-dee5-4834-9d98-8f9c07f0a602/9781000567113.pdf

ESET (2025) APT report: Russian cyberattacks in Ukraine intensify – Sandworm unleashes new destructive wiper. Available online: https://www.globenewswire.com/news-release/2025/05/20/3085225/0/en/ESET-Research-APT-Report-Russian-cyberattacks-in-Ukraine-intensify-Sandworm-unleashes-new-destructive-wiper.html

Gartzke, E., and Lindsay, J. R. (2017) Thermonuclear cyberwar. *Journal of Cybersecurity*, 3(1): 37–48. Available online: https://academic.oup.com/cybersecurity/article/3/1/37/2996537

Giles, K. (2017) Countering Russian information operations in the age of social media, Council for Foreign Relations. Available online: https://www.cfr.org/report/countering-russian-information-operations-age-social-media

Giles, K. (2023) Russian cyber and information warfare in practice. Chatham House. Available online: https://www.chathamhouse.org/2023/12/russian-cyber-and-information-warfare-practice/03-distinctive-features-war

Goldsmith, S., and Eggers, W. D. (2004) Governing by Network: The New Shape of the Public Sector. Brookings Institution Press.

Google Cloud (2024) APT44: Unearthing Sandworm. Available online: https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf

Greenberg, A. (2018) The untold story of NotPetya, the most devastating cyberattack in history. Wired. July 9. Available online: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Gunderman, D. (2022) Report: DHS Fears Russian Cyberattack If US Acts on Ukraine. *GovInfo Securtity*. January 24. Available online: https://www.govinfosecurity.com/report-dhs-fears-russian-cyberattack-if-us-acts-on-ukraine-a-18370

GUR (2024) Software, Ciphers, Secret Documents — DIU Cyber Specialists Hacked Russia's Defence Ministry. March 4. Available online: https://gur.gov.ua/en/content/soft-shyfry-sekretni-dokumenty-kiberfakhivtsi-hur-zlamaly-minoborony-rosii.html

Harding, L. (2022) Ukraine's publicised southern offensive was disinformation campaign. *The Guardian*. September 10. Available online: https://www.theguardian.com/world/2022/sep/10/ukraines-publicised-southern-offensive-was-disinformation-campaign

Helmund, T., and Holynska, K. (2024), Ukrainian Resistance to Russian Disinformation, RAND. September 3 2024. Available online: https://www.rand.org/pubs/research_reports/RRA2771-1.html

Horowitz, M. C. (2010) The Diffusion of Military Power: Causes and Consequences for International Politics. Princeton: Princeton University Press.

Hunder, M. (2024) Russia vs Ukraine: The biggest war of the fake news era. *Reuters*. August 1. Available online: https://www.reuters.com/world/europe/russia-vs-ukraine-biggest-war-fake-news-era-2024-07-31/

Huxham, C., and Vangen, S. (2005) Managing to Collaborate: The Theory and Practice of Collaborative Advantage. Abingdon: Routledge.

Iyengar, R. (2022) U.S. Braces for Russian Cyberattacks as Tensions With Ukraine Escalate. *CNN*. February 24. Available online: https://edition.cnn.com/2022/02/24/tech/russia-ukraine-us-sanctions-cyberattacks

Kello, L. (2013) The meaning of the cyber revolution: Perils to theory and statecraft. *International Security*, 38(2): 7–40. Available online: https://direct.mit.edu/isec/article/38/2/7/12094/The-Meaning-of-the-Cyber-Revolution-Perils-to

Kirichenko**,** D. (2025) Ukraine's IT Army is Waging a Crowdsourced Cyber War Against Russia. *Small Wars Journal*. March 24. Available online: https://smallwarsjournal.com/2025/03/24/ukraines-it-army-is-waging-a-crowdsourced-cyber-war-against-russia/

Kyiv Independent (2024) Military intelligence claims cyberattack on Russian defense ministry gave access to classified documents. Available online: https://kyivindependent.com/military-intelligence-claims-cyberattack-on-russian-defense-ministry-gave-access-to-classified-documents/

Kyiv Post (2024a) HUR Initiates Cyberattack on Russian Drone Control Programs. February 8. Available online: https://www.kyivpost.com/post/27795

Kyiv Post (2024b) Ukrainian Hackers Launch Cyberattacks on Moscow Sewage System – Sources. June 19. Available online: https://www.kyivpost.com/post/30890

Kyiv Post (2024c) HUR Hackers Score Cyber-Hit on Russian Airports, Cause Flight Delays. August 15. Available online: https://www.kyivpost.com/post/34195

Liebetrau, T. (2022) Organizing cyber capability across military and intelligence entities: collaboration, separation, or centralization. *Policy Design and Practice*. 6(2): 131–145. https://doi.org/10.1080/25741292.2022.2127551

Libicki, M. C. (2007) Conquest in Cyberspace: National Security and Information Warfare. Cambridge University Press.

Lindsay, J. R. (2013) Stuxnet and the limits of cyber warfare. *Security Studies*, 22(3): 365-404. Available online: https://www.tandfonline.com/doi/abs/10.1080/09636412.2013.816122

Linvil, D, and Warren, P. (2025) Ukraine: The Past, Present, and Future of Russian Disinformation. Lawfare. Available online: https://www.lawfaremedia.org/article/ukraine--the-past--present--and-future-of-russian-disinformation

Mandiant (2023) The GRU's disruptive playbook. Google Cloud Blog. July 12. Available online: https://cloud.google.com/blog/topics/threat-intelligence/gru-disruptive-playbook

Maschmeyer, L. (2021) The subversive trilemma: Why cyber operations fall short of expectations. *International Security*, 46(2): 51–90.

Melella, C., Ferazza, F., and Mersinas, K. (2024) Disjointed Cyber Warfare: Internal Conflicts among Russian Intelligence Agencies. *ACIG*, 3(2): 38–71. Available online: https://www.acigjournal.com/Disjointed-Cyber-Warfare-Internal-Conflicts-among-Russian-Intelligence-Agencies,192120,0,2.html

Meta (2022) Removing coordinated inauthentic behavior from China and Russia. Meta Newsroom. September 27. Available online: https://about.fb.com/news/2022/09/removing-coordinated-inauthentic-behavior-from-china-and-russia/

Microsoft (2022) Defending Ukraine: Early lessons from the cyber war. June 22. Available online: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/

Microsoft (2025) The BadPilot campaign: Seashell Blizzard subgroup conducts multiyear global access operation. February 12. Available online: https://www.microsoft.com/en-us/security/blog/2025/02/12/the-badpilot-campaign-seashell-blizzard-subgroup-conducts-multiyear-global-access-operation/

Miller, M. (2022) Russian invasion of Ukraine could redefine cyber warfare. *Politico*. January 28. Available online: https://www.politico.com/news/2022/01/28/russia-cyber-army-ukraine-00003051

Miller, M. (2025) Ukraine's IT Army is Waging a Crowdsourced Cyber War Against Russia. *Small Wars Journal*. Available online: https://smallwarsjournal.com/2025/03/24/ukraines-it-army-is-waging-a-crowdsourced-cyber-war-against-russia/

Mumford, A. (2013) Proxy Warfare. Oxford: Polity Press. National Cyber Security Centre (NCSC), National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), & Canadian Centre for Cyber Security (CNMF) (2023, September) Infamous Chisel – Sandworm's Android malware used against Ukraine. Available online: https://www.cyber.gc.ca/en/news-events/joint-report-new-russian-malware-campaign-targeting-ukrainian-military

NATO StratCom Centre of Excellence (2023) Countering Disinformation: Institutional Gaps and Strategic Options. Riga: NATO StratCom COE.

News.com.au (2024) Nothing secret left: Ukraine hacks its way to crucial Russian military information in huge blow to Vladimir Putin. Available online: https://www.news.com.au/world/europe/nothing-secret-left-ukraine-hacks-its-way-to-crucial-russian-military-information-in-huge-blow-to-vladimir-putin/news-story/9603f57dccf52956cad41b0808898062

NSA (2025) NSA and others publish advisory warning of Russian state-sponsored cyber campaigns. May 14. Available online: https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4193749/nsa-and-others-publish-advisory-warning-of-russian-state-sponsored-cyber-campai/

Olson, M., and Zeckhauser, R. (1966) An economic theory of alliances. *The Review of Economics and Statistics*, 48(3): 266–279. Available online: https://www.jstor.org/stable/1927082

Oosterveld, W., Wojcik, A., and Brandsma, L. (2023) Meme Warfare in the Russia-Ukraine War: Humour as a Tool of Digital Influence. *arXiv*. Available online: https://arxiv.org/pdf/2309.08363.pdf

Pamment, J. (2022) A Capability Definition and Assessment Framework for Countering Disinformation, Information Influence, and Foreign Interference, NATO Strategic Communications Centre of Excellence. Available online: https://stratcomcoe.org/pdfjs/?file=/publications/download/Defining-Capabilities-DIGITAL.pdf

Paul, C., and Matthews, M. (2016) The Russian "firehose of falsehood" propaganda model: Why it might work and options to counter it. Rand Corporation. Available online: https://www.rand.org/pubs/perspectives/PE198.html

Posen, B. R. (1984) The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars. Ithaca: Cornell University Press.

Potti, D. (2024) Inside Ukraine's New Digital Defense Strategy to Counter Russian Cyber Onslaught.U24 May 18. Available online: https://united24media.com/opinion/inside-ukraines-new-digital-defense-strategy-to-counter-russian-cyber-onslaught-7747

RAND Corporation (2024) Russia's War in Ukraine: Emerging insights for UK and NATO joint doctrine. Available online: https://www.rand.org/randeurope/research/projects/2024/russias-war-in-ukraine-insights-for-uk-and-nato.html

Remnick, D. (2022) Putin's Preparation for Ukraine. *The New Yorker*. February 21. Available online: https://www.newyorker.com/news/daily-comment/putins-preparation-for-ukraine

Renden-Katolik A. (2023) The IT Army of Ukraine. *CSIS*. August 15. Available online: https://www.csis.org/blogs/strategic-technologies-blog/it-army-ukraine

Rid, T. (2020) Active Measures: The Secret History of Disinformation and Political Warfare. New York: Farrar, Straus and Giroux.

Rid, T. (2011) Cyber war will not take place. *Journal of Strategic Studies*, 35(1): 5–32. Available online: https://www.tandfonline.com/doi/abs/10.1080/01402390.2011.608939

RNBO (2025) Activities. National Security and Defense Council of Ukraine. Available online: https://rnbo.gov.ua/en/Diialnist/7169.html

Robertson, A. (2025) Ukraine's Operation Spiderweb shows how drone strikes are now media campaigns too. *The Verge*. June 3. Available online: https://www.theverge.com/politics/678329/ukraine-drone-strike-attack-videos-social-media-russia

Rosen, S. P. (1991) Winning the Next War: Innovation and the Modern Military. New York: Cornell University Press.

Sanger, D. E. (2018) The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age. New York: Crown.

Sapolsky, H. M., Friedman, B. H., and Green, B. R. (Eds.) (2009) US Military Innovation Since the Cold War: Creation Without Destruction. Oxford: Routledge.

Schectman, J., and Bing, C. (2022). EXCLUSIVE Ukraine calls on hacker underground to defend against Russia. *Reuters*. February 21. Available online: https://www.reuters.com/world/exclusive-ukraine-calls-hacker-underground-defend-against-russia-2022-02-24/

Schnurr, L. (2025) The Fight Against Disinformation: A Persistent Challenge for Democracy. Foreign Policy Research Institute (FPRI). January 5. Available online: https://www.fpri.org/article/2025/01/the-fight-against-disinformation-a-persistent-challenge-for-democracy

Schulze, M. (2024, October) Hacking the cosmos: Cyber operations against the space sector – A case study from the war in Ukraine. CSS ETH Zurich. Available online: https://css.ethz.ch/en/center/CSS-news/2024/10/hacking-the-cosmos-cyber-operations-against-the-space-sector-a-case-study-from-the-war-in-ukraine.html

Sherman, J. (2025) Unpacking Russia's cyber nesting doll, Atlantic Council. 20 May. Available online: https://www.atlanticcouncil.org/content-series/russia-tomorrow/unpacking-russias-cyber-nesting-doll/

Smeets, M. (2018) The strategic promise of offensive cyber operations. *Strategic Studies Quarterly*, 12(3): 90–113. Available online: https://www.jstor.org/stable/26481911

SWP (2023) Cyber Operations in Russia's War against Ukraine. Stiftung Wissenschaft und Politik. Available online: https://www.swp-berlin.org/10.18449/2023C23/

The Times (2024) How Ukraine is waging information warfare to outwit Russians. Available online: https://www.thetimes.com/world/russia-ukraine-war/article/how-ukraine-is-waging-information-warfare-to-outwit-russians-5zn3fxlmm

United24 Media (2024) Palantir: The secretive tech giant shaping Ukraine's war effort. April 5. Available online: https://united24media.com/war-in-ukraine/palantir-the-secretive-tech-giant-shaping-ukraines-war-effort-5519

UNN (2024) Ukrainians Hacked Russian Program for Drone Control – DIU. February 8. Available online: https://unn.ua/en/news/ukrainians-hacked-russian-program-for-drone-control-diu

U.S. Department of Defense (2025) Russian GRU Targeting Western Logistics Entities and Technology Companies. May 21. Available online: https://media.defense.gov/2025/May/21/2003719846/-1/-1/0/CSA_RUSSIAN_GRU_TARGET_LOGISTICS.PDF

U.S. Senate Select Committee on Intelligence (2019) Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Vol. 2. Washington, DC: U.S. Government Publishing Office.

Valeriano, B., and Maness, R. C. (2015) Cyber War versus Cyber Realities: Cyber Conflict in the International System. New York: Oxford University Press.

Wanless, A., and Berk, M. (2021) The changing nature of propaganda: Coming to terms with influence in conflict, The World Information War. Available online: https://www.taylorfrancis.com/chapters/edit/10.4324/9781003046905-7/changing-nature-propaganda-alicia-wanless-michael-berk

Wilde, G. (2024) Technology Alone Won't Break the Stalemate in Ukraine, Foreign Policy. March 19. Available online: https://foreignpolicy.com/2024/03/19/technology-ai-drones-stalemate-ukraine-russia-manpower/

Wilner, A. S., Williams, G., Thuns-Rondeau, M., Beaulieu, N., and Cossette-Sharkey, V. (2024) Offensive cyber operations and state power: Lessons from Russia in Ukraine. *International Journal*, 79(2): 123–142. Available online: https://vlex.co.uk/vid/offensive-cyber-operations-and-1039301020

AUTHOR

William Dixon holds a Master's Degree in Intelligence and International Security from the War Studies Department of King's College London (UK), and is an Associate Fellow at the Royal United Services Institute (RUSI) (London, UK) and a Senior Tech and Cyber Fellow at the Ukraine Foundation (Geneva, Switzerland). He is an expert in cyber security and international relations, with a focus on military innovation and digital conflict. He was formerly a Head at the World Economic Forum's Centre for Cybersecurity and started his career at the UK's Cyber and Signals Intelligence Agency – Government Communication's Headquarters (GCHQ). Email: williamjamesdixon@gmail.com