



ISSN: 1060-586X (Print) 1938-2855 (Online) Journal homepage: www.tandfonline.com/journals/rpsa20

The invisible front: Ukraine's IT army and the evolution of cyber resistance

Anna Lysenko & Seva Gunitsky

To cite this article: Anna Lysenko & Seva Gunitsky (15 May 2025): The invisible front: Ukraine's IT army and the evolution of cyber resistance, Post-Soviet Affairs, DOI: [10.1080/1060586X.2025.2503658](https://doi.org/10.1080/1060586X.2025.2503658)

To link to this article: <https://doi.org/10.1080/1060586X.2025.2503658>



Published online: 15 May 2025.



Submit your article to this journal [↗](#)



Article views: 31



View related articles [↗](#)



View Crossmark data [↗](#)



The invisible front: Ukraine's IT army and the evolution of cyber resistance

Anna Lysenko and Seva Gunitsky

Department of Political Science, University of Toronto, Toronto, Canada

ABSTRACT

Russia's invasion of Ukraine in 2022 saw the emergence of a new actor: the IT Army of Ukraine (ITAU), a volunteer cyber force that countered Russian disinformation and targeted its digital spaces. We argue that the ITAU contributed to Ukraine's political victory in the Battle of Kyiv by projecting national resilience to both domestic audiences and international observers. By countering Russian cyberattacks and mounting its own offensive campaigns, the ITAU not only disrupted enemy capabilities but also bolstered domestic morale and helped shape global perceptions of Ukraine's ability to defend itself. This resistance contributed to Ukraine's overall hybrid resilience in the crucial opening months of the invasion. More broadly, the ITAU reflects a growing shift in cyber conflict away from covert technical sabotage toward visible, politically charged campaigns aimed at controlling narratives and influencing perceptions. As a key case study of civilian cyber-mobilization, the ITAU offers broader insights into the evolving role of civilian participation in future conflicts.

ARTICLE HISTORY

Received 22 August 2024
Accepted 20 April 2025

KEYWORDS

Russia-Ukraine war; internet army; cyber conflict; non-state actors in cyberspace

The opening days of Russia's 2022 invasion of Ukraine saw the creation of an unprecedented wartime actor: the IT [Internet] Army of Ukraine (ITAU). The IT Army became the world's first organized online force to mobilize against an enemy invasion. Endorsed and supported by the Ukrainian government, the group brought together volunteer hackers, mostly Ukrainian, some located inside physical war zones, who worked to target Russian online infrastructure and counter Russian disinformation efforts.

One such war zone was the Battle of Kyiv, lasting from February 24 to March 29, in which Ukraine achieved an important early victory by resisting Russia's military advance. In that fight the country also achieved a political victory: its robust physical and cyber resistance to Russia demonstrated to both domestic audiences and the international community that it remained a resilient sovereign state.

This paper examines the role of the ITAU in contributing to Ukraine's successful resistance in the early days of the invasion. Beyond countering Russian cyberattacks and disinformation campaigns, the ITAU adopted an offense-minded "attack-to-defend" cyber strategy. As part of the resistance, the ITAU disrupted networks, attacked

CONTACT Seva Gunitsky  s.gunitsky@utoronto.ca  Department of Political Science, University of Toronto, Toronto, Canada

This article was originally published with errors, which have now been corrected in the online version. Please see Correction (<http://dx.doi.org/10.1080/1060586X.2025.2509377>)

© 2025 Informa UK Limited, trading as Taylor & Francis Group

symbolically important Russian sites via distributed denial-of-service (DDoS) attacks, and inserted pro-Ukrainian messages into Russian online communities.

By early June 2022, this strategy had resulted in ITAU directing 662 targeted DDoS targets against Russian government and corporate websites (Soesanto 2022). The direct effect was to divert Russian resources away from warfare and towards defending against the ITAU's attacks. More indirectly, the ITAU's emergence channeled and maintained domestic morale during the difficult initial period of the invasion, and positively influenced international perceptions of what we call Ukraine's "hybrid resilience."

We define hybrid resilience as the ability to withstand simultaneous attacks across a range of domains, not only in the sphere of military conflict but also cyberattacks, disinformation, and public perception. Ukraine's demonstration of this multi-domain resilience was key for maintaining both its domestic cohesion and international support in the early stages of the invasion. The ITAU played a vital role in contributing to that hybrid resilience. Its emergence sent a credible signal to Western audiences that the country as a whole was committed to defending against the conquest. As the former White House cyber co-ordinator for President Obama put it shortly after the ITAU began operations: "Part of it is also a signaling exercise. It's signaling a level of commitment across the country of Ukraine to resisting what the Russians are doing" (Burgess 2022).

Through a combination of cyberattacks, disinformation counter-strategies, and public engagement, the ITAU not only helped to secure a tactical advantage over Russian forces but also played a pivotal role in shaping the narrative of the war domestically and abroad. The ITAU's unusual role and tactics highlight the evolving nature of modern conflict, showcasing the increasing importance of intangible sources of power alongside conventional military assets. More generally, the strategic use of the ITAU by the Ukrainian government serves as an important case study of modern hybrid warfare, illustrating how states can leverage cyber capabilities to find new and unexpected sources of support during crises and conflicts. Examining the role of novel actors like the ITAU will thus become increasingly important for understanding modern conflict.

The ITAU emerged in a context of widespread expectations of significant Russian cyberattacks in February 2022, similar to those experienced by countries such as Georgia in 2008. But these devastating attacks never fully materialized. Multiple factors explain this outcome, including poor Russian coordination and effective Ukrainian defenses. Civilian cyber-mobilization, exemplified by the ITAU, could offer a cost-effective defense for states with limited resources. Yet it also faces significant challenges such as coordination inefficiencies, unclear command structures, and legal ambiguities.

In its operations, the ITAU represents a clear instance of "participative warfare," in which digital technology facilitates civilian involvement. This trend has blurred traditional lines between civilians and combatants, raising complex legal and ethical questions. Consistent with the emerging literature, the ITAU exemplifies a broader shift in cyber warfare from clandestine attacks to large-scale public information warfare, focusing on countering propaganda and influencing global narratives rather than just causing network disruptions.

One advantage of using the ITAU as a case study is its public-facing character. In contrast to the usual secrecy of cyber warfare, the ITAU conducted its operations openly and transparently, with the goals of demoralizing the enemy, influencing public conversations, and garnering support both at home and abroad. Cyber activity is often difficult

to investigate because of its shrouded and anonymized nature. By contrast, the ITAU's campaigns were announced publicly, which aided in our analysis. We use primary online sources to analyze cyberattacks and anti-disinformation campaigns confirmed to have been launched by the ITAU during the Battle of Kyiv. This analysis is based on the ITAU's official channels, most prominently on Ukrainian- and Russian-language Telegram, as well as government documents and other media and social media reports.

The remainder of the paper proceeds as follows. The first section situates the group's origins and activities within the broader literature on modern cyber conflict, focusing on the evolving role of non-state actors and civilian mobilization in wartime. We then briefly review Russian and Ukrainian cyber capabilities prior to 2022. The rest of the paper examines the ITAU's role in the Battle of Kyiv, focusing on the group's targeting of Russian government websites and campaigns against disinformation. These activities not only imposed direct costs on Russia but also promoted Ukraine's narrative and resilience to domestic and international audiences.

ITAU and civilian cyber-mobilization in wartime

While unprecedented in important ways, the IT Army of Ukraine did not emerge in a vacuum. This section examines the group's creation and operations in the broader context of modern cyber conflict, focusing on the evolving role of non-state actors and civilian mobilization in wartime.

Research on the cyber dimensions of Russia's invasion has identified several features of the conflict that help explain the emergence and operations of the ITAU. One is the widespread pre – February 2022 expectation of a Russian “cyber-blitzkrieg” – a devastating series of online attacks that would accompany the physical invasion (Givens, Gorbachevsky, and Biernat 2023; Kostyuk and Gartzke 2022; Lin 2022). As Brantly and Brantly (2024, 475) note, the invasion “was expected to bring with it a commensurate escalation in ‘hybrid’ or cyber tactics.” This expectation was bolstered by previous Russian conduct in places like Georgia, where in 2008 the physical fighting was accompanied by coordinated cyberattacks (Beehner et al. 2018). A key factor behind ITAU's creation, therefore, was the expectation of such attacks from Russia, coupled with uncertainty about Ukraine's ability to defend itself in the digital domain.

Despite these expectations, a Russian cyber Pearl Harbor did not materialize. As a number of scholars have argued, Russian cyberattacks have not been a significant factor in the conflict since 2022. Kostyuk and Brantly (2022), for instance, note that none of Russia's attacks “significantly impacted the ability of Ukraine to conduct military operations or communicate effectively with external partners and by extension did not have any strategic impact on Ukraine's warfighting capabilities” (Kostyuk and Brantly 2022, 498).¹

How to explain this gap between expectation and reality? The literature on the subject has produced several explanations. One perspective attributes the lack of major Russian cyberattacks to poor coordination, stemming in part from Moscow's expectation of a short conflict (Casey and Gunitsky, 2022; Schulze and Kerttunen 2023). Another has been to highlight the effectiveness of Ukraine's cyber defenses, including both state efforts and civilian contributions.² Givens, Gorbachevsky, and Biernat (2023, 97), for instance, argue that “impressive Ukrainian cyber defense measures have blunted

[Russian] attacks, contrary to predictions expressed by some Western intelligence services, technology firms, and scholars.”³

While the reasons behind a lack of destructive cyberattacks are multicausal, the ITAU was well positioned to play a contributing role in this successful defense by mobilizing tens of thousands of volunteers to disrupt Russian digital infrastructure and information campaigns.⁴ Despite Russian efforts, Ukraine’s cyber defenses – bolstered by government coordination and civilian contributions – have largely withstood Russian cyber aggression, and the ITAU’s existence helps to explain that outcome.

Another response to the lack of a Russian cyber-blitzkrieg since 2022 has been to reconsider the nature or purpose of cyberwarfare itself. Scholars such as James Lewis (2022) argue that the conflict demonstrates the “overrated” strategic value of cyberwar. This strand of scholarship argues that rather than directly shaping battlefield outcomes, cyber operations are most effective when focusing on intelligence gathering, deception, and political warfare. Kostyuk and Gartzke (2022), for instance, argue that cyber conflict is primarily about winning information contests rather than replacing conventional military force. In the Russia-Ukraine war, they suggest, cyber operations have played a more significant role in shaping narratives and public perception than in causing physical destruction.

In line with these arguments, the ITAU’s operations exemplify a shift in the nature of cyberwarfare. The group’s focus on disrupting propaganda and broadcasting pro-Ukrainian messages illustrates how cyber operations have evolved from clandestine attacks on enemy infrastructure to influencing public opinion and framing the conflict’s broader narrative to foreign and domestic audiences. The group’s visibility and open participation present a clear contrast to the secrecy of traditional cyberwar. This approach underscores a key evolution in cyber conflict: a move from shadowy cyberattacks toward large-scale information warfare (Mueller et al. 2023). By operating publicly, the ITAU aimed to demoralize adversaries, shape global discourse, and rally international support.

The ITAU’s role in the war also demonstrates the increasing involvement of non-state actors in modern conflict. Even prior to 2022, the Russia-Ukraine war served as an example of what Merrin (2018) calls “participative warfare,” characterized “by the integration of various non-traditional actors into the conflict space, facilitated by advancements in technology and communication networks” (Norman 2024).⁵ By lowering the barriers for wartime engagement, participative warfare allows more citizens to actively support the national effort, but also blurs the distinction between civilians and combatants.

Created by volunteers but with active government engagement, the ITAU’s existence embodies the concept of “participative warfare” by challenging traditional distinctions between state and non-state actors. In doing so it raises questions about the legal and ethical implications of civilian participation in modern warfare, the effectiveness of decentralized cyber militias, and the long-term viability of such models for state defense strategies.⁶ The ITAU’s ability to emerge and operate was made possible by its integration with the Ukrainian government, yet maintaining its decentralized nature allows it to remain flexible and adaptable. While the legal and ethical implications are murky, Ukraine’s defense strategy demonstrates the increasing role of non-state actors and decentralized operations in modern conflict.⁷

Civilian mobilization in conflict

The mobilization of civilians in times of war is not a new phenomenon, but the ITAU presents a unique case of a state encouraging the creation of a large-scale, decentralized volunteer cyber force. In fact, the participatory and online nature of modern cyber conflict readily facilitates the incorporation of civilian resources. The ITAU's emergence thus highlights what Wheat and Kirichenko (2024) have dubbed the "democratization of irregular warfare." Looking at the Russia- Ukraine war, they note that technological advancements have enabled ordinary citizens to participate directly in modern conflicts. This participation extends beyond information warfare. The proliferation of affordable drones, for example, has allowed civilians to conduct reconnaissance and even execute attacks, roles that were once exclusive to military forces (Ford 2024).⁸

The peculiar democratization of warfare is especially significant in the digital realm. With cyberattacks, individuals and small groups can disrupt enemy communications, gather intelligence, and spread disinformation. Social media platforms have become powerful civilian tools for influence operations, enabling non-combatants to shape public opinion, both domestically and internationally (Singer and Emerson 2018). The ITAU's participatory and decentralized nature thus offers a vivid example of this lowering of barriers to entry in modern war.

The large-scale involvement of civilians in cyber and information warfare thus presents a new dimension of contemporary conflict. Given Russia's proclivity for "hybrid warfare" and history of past aggression to its neighbors, it is not surprising that states around Russia have previously turned to civilian mobilization in information warfare. As a civilian cyber-defense force created in response to Russian aggression, the ITAU found a precedent Estonia's Cyber Defense Unit (CDU), established in 2011 after Russian cyber-attacks on Estonian infrastructure (Grzegorzewski, Smith, and Koven 2023; Kaska, Osula, and Stinissen 2013). Like the ITAU, the CDU is comprised of civilian volunteers who assist the government in defending critical digital assets during crises. The push to create the ITAU was thus consistent with a prevailing regional belief in Russia's offensive cyber-capabilities and its history of past attacks. Because these conditions are likely to persist, we may expect more groups like the CDU and the ITAU to be mobilized in response to – or in anticipation of – Russian hostilities.

Battles over information narratives naturally lend themselves to civilian participation and mobilization. Cyber-mobilization also offers a relatively low-cost way to engage a population in national defense without requiring them to take up arms. Compared to conventional military mobilization, crowd-sourced cyber operations require fewer resources, making them an appealing tool for states with limited defense budgets. However, this model also has its limitations. Operating with decentralized methods offers flexibility but can lead to inefficiencies in coordination, target selection, and execution.

Unlike traditional military units, which operate under a clear hierarchy, the ITAU largely coordinates through Telegram channels and other digital communication tools (Braw 2022). While this structure allows for adaptability and speed, the absence of a formal chain of command means that decision-making is fluid and ad hoc, which can be both an advantage and a vulnerability. States that encourage civilian mobilization in the cyber realm face several challenges. A major concern is the legitimacy and effectiveness of decentralized groups. Without a clear command structure, coordination can be difficult,

leading to inefficiencies or even counterproductive actions. Moreover, legal issues arise when volunteers engage in cyberattacks, as international law does not clearly define the role of civilian hackers in armed conflicts (Kirichenko 2023). The blurred line between state and civilian efforts complicates questions of accountability and responsibility in cyber warfare.

The ITAU's emergence also fits within a broader pattern of civilian mobilization in Ukraine over the past few years. For example, Stepaniuk (2022) has highlighted the importance of informal networks and private-sector resources for large-scale civilian mobilization in Ukraine. The rise of digital platforms has further expanded opportunities for decentralized civilian engagement, allowing for rapid communication, recruitment, and coordination.

In the context of modern conflict, resilience against hybrid warfare requires not only military strength but also the social capacity to organize and resist through various means, including cyber efforts. Hybrid resilience involves maintaining domestic cohesion, securing international support, and demonstrating the will to resist aggression.⁹ The ITAU's formation aligns with this broader resilience-building strategy by showcasing how civilian engagement can complement state efforts in defense and information warfare. As information warfare continues to evolve, the role of civilian mobilization will likely expand, reshaping conventional military strategies.

Given these trends, the ITAU provides an especially useful case study for understanding how states can leverage civilian resources in the digital domain, and how these efforts shape modern warfare. While the ITAU represents a novel model of civilian cyber-mobilization, its emergence and operations are also linked to broader ongoing developments in cyber conflict. In this way, the ITAU demonstrates the evolving role of cyberwarfare and the changing nature of civilian mobilization in modern war.

Russian and Ukrainian cyber capabilities prior to 2022

Both Ukraine and Russia had formidable cyber capabilities before the full-scale invasion. Unlike Ukraine, however, the Russian government had been increasingly co-opting its illicit agents toward participation in pro-government activity. The Putin regime tacitly supported its cyber criminals as early as 2010, so long as they did not attack the state or other Russian targets. During the 2010s, Russian malicious cyber activity had been documented in Estonia, Georgia, Crimea, the US, and Europe (Levyatan 2022). Moscow has consistently denied these connections even as it has developed an international reputation as an aggressive cyber power alongside actors such as North Korea and Iran (Carlin and Graff 2018, 21; Shead 2022). Russia's cybersecurity posture has remained somewhat elusive by design, but its strong offensive cyber capabilities suggested it also had significant cyber defenses in place (Voo et al. 2020; Wolff 2022).

Like Russia, Ukraine's strong scientific and technological education, economic challenges, and weak social norms, especially regarding criminal activity after the collapse of the Soviet Union, produced an environment conducive to hackers (Kostyuk 2015). Ukraine developed an influential (if somewhat chaotic) cyberspace, with Ukrainian hackers also often working independently to attack targets in the US and Europe, most often for financial gains. Since the 2014 Crimea annexation, the Ukrainian government has made progress in digitizing the country and improving cybersecurity, especially that of critical

infrastructure. With significant political and economic support from the US and the EU, Ukraine was able to make notable progress in improving its cyber legislation, with anti-corruption measures and foreign oversight (Kostyuk 2015, 121; Shopina et al. 2020). It created the Ministry of Digital Transformation in 2019 to further support domestic startups and attract global tech companies to collaborate with and invest in Ukraine's growing industry (Bornyakov and Labott 2022).

Climbing toward cyberconflict

These pre-2022 developments laid the foundation for the ITAU's emergence. By January 2022, Russia had amassed over 100,000 troops on Ukraine's borders. The lead-up to the invasion was hotly contested within and beyond Ukraine: many international experts claimed Ukraine would be conquered by Russia within weeks if not days (Fix and Kimmage 2022, Nagl 2022). Similarly, experts warned that Ukraine would be incapacitated by unprecedented cyberattacks, thereby making Russia's invasion even more harrowing and anarchic for those who would lose critical infrastructure access and online communication (Miller 2022a, Nakashima and Horton 2022).

In fact, cyberspace did serve as a harbinger for the general invasion, as a series of large-scale attacks damaged Ukraine's governmental, private, and public sectors in mid-January (Neuman, 2025). While Ukraine had grown accustomed to Russian cyberattacks, these were notable for their unprecedented scale and destructive capabilities. On 23 February, hours before the physical invasion began, researchers at the cybersecurity firm ESET (2022) found destructive software circulating in hundreds of Ukrainian computers. The malware wiped data from the devices it infected, although the exact type and content of the data lost was unspecified. The victims included a Ukrainian government agency and a financial institution (Pearson 2022a). This attack was set up in such a way that hackers needed to have prior access to the domain, indicating that Russians had been spying on Ukrainian systems for months before the attacks (Reuters 2022).

In response, Ukraine's government released a statement: "Moscow continues to wage a hybrid war and is actively building up its forces in the information and cyberspaces . . . not just to intimidate society, but to destabilize the situation in Ukraine by stopping the public sector's work and undermining Ukrainians' confidence in their government" (Karmanau 2022). Thus, even before the invasion officially began, Ukraine had acknowledged cyberconflict as an important domain of any future warfare (Neuman, 2025).

The next step in this escalation was the Viasat hack, marking the start of the full-scale Russia-Ukraine cyberconflict. A massive cyberattack against the American communications company Viasat began hours before the physical invasion on 24 February. Russians accessed the network and inserted malware that made tens of thousands of modems in Ukraine lose internet connection, with parts of Central Europe also affected. Investigators found the initial breach was due to a single misconfigured device, which likely allowed the hackers to gain entry (Mathews 2022). Regarding the attack's impact, former deputy chief Victor Zhora would later say this caused "a really huge loss in communications in the very beginning of war" (Shead 2022). The Viasat outage remains the largest publicly known cyberattack to take place during Russia's full-scale invasion.

A number of observers expected Russia to initiate a cyber "Pearl Harbor" in the months and days leading up to the invasion (Miller 2022a, Nakashima and Horton 2022). However,

like its initial physical assault, the actual demonstration of Russia's CyberPower was underwhelming. Attacks against the Ukrainian military and governmental sectors increased by 196% in the three days following the invasion (Check Point Research Team 2022). Yet only the Viasat attack was considered an attack of significant scale and threat, with its impact diffusing beyond Ukraine's borders (Carvin 2022).

While Russia has launched numerous cyberattacks since 2022, so far Ukraine's critical infrastructure and networks have not been affected as much as experts expected (Miller 2022b). One possibility for the war remaining mostly physical is that Russia's government did not think it required preparation to overcome Ukraine, or did not find opportunities to prepare coordinated physical and digital attacks. Another possibility, offered by Ukrainian government officials and scholars, was that Russia was trying to mount more damaging attacks but was being prevented from doing so by the Ukrainian government's cyber defences and the ITAU (Bateman, Beecroft, and Wilde 2022; Security Service of Ukraine 2022b).

The battle of Kyiv begins

On 24 February 2022, Russian missiles struck major cities including Kyiv, Kharkiv, Mariupol, Odesa, Donetsk, and Luhansk. Tanks and troops rolled in from Ukraine's north, east, and south, by all appearances converging upon Kyiv. In the fog of war, Ukrainian authorities urged the population to stay calm while the Armed Forces raced into battles.

In the early fog of the invasion, Russian-produced disinformation briefly flourished. One prominent rumor was that President Volodymyr Zelenskyy had fled the country; this was debunked by Zelenskyy filming himself with his close cabinet advisers outside in Kyiv (Garber 2022). There were also widespread worries of Russian cyberattacks blocking communications, as they had partially done in the Viasat attack. However, the country's leadership appeared determined to fight back. To quote President Zelenskyy's speech from a few hours before the invasion, "We know for sure that we do not need war. Not a Cold War, not a hot one, not a hybrid one. . . . When you attack us, you will see our faces, not our backs" (Guardian News 2022).

As Russians approached Kyiv over the next few days, Ukraine's army and thousands of newly created combat volunteer units set up defenses. Former Commander-in-Chief of the Armed Forces of Ukraine Valerii Zaluzhnyi reported that over 37,000 people volunteered to join the Ukrainian Armed Forces (Beliakova 2022; TSN 2022). The B.B.C. reported that around 18,000 of those Ukrainians volunteered to defend Kyiv, with some civilians even being turned away due to a lack of weapons (Zitser 2022). This physical mobilization demonstrated, domestically and internationally, Ukrainians' determination to defend themselves with limited resources against a formidable opponent.

A similar patriotic sentiment resulted in the ITAU. Decentralized in form yet unified in purpose, the ITAU became the world's first spontaneous cyber army. It is perhaps fitting that as a civilian-driven group, the ITAU originated as the idea of one entrepreneurial Ukrainian. The first call for a "hacktivarney" was made on Facebook by Yegor Aushev, the founder of the Ukrainian cybersecurity company Cyber Unit Technologies, which had worked with Ukraine's government to protect critical infrastructure (Schectman and Bing 2022). He wrote on Facebook on 25 February, stating "The time has come to maximize the cyber protection of our country." Volunteers could sign up for this army through a Google

form, which asked about their cyber experience, what field they specialized in, and if they wanted to be involved in attack or defense. They also needed to provide a Ukrainian contact of reference who could attest to their experience and character (Schectman and Bing 2022). Aushev also stated, “If Kyiv falls, we keep hacking Putin” (T. Brewster 2022a). This commitment to cyberattacks paralleled statements by Kyiv’s volunteer battalion fighters in the Battle of Kyiv, with one volunteer declaring, “We will fight as much as we can . . . we are not ready to give up” (D’Agata, Redman, and Ott 2022).

The official ITAU was formed only a few days later, with Aushev working with the Ukrainian government to foster his initiative (Schectman and Bing 2022). On 26 February 2022, at 8:38 p.m. Kyiv time, the Minister of Digital Transformation Mykhailo Fedorov posted a Telegram message that read “We are creating an IT army. We need digital talents” (Fedorov 2022; Shead 2022). On 28 February 2022, the Security Service of Ukraine (2022a) Tweeted “CYBER FRONT IS NOW OPEN! Help Ukrainian cyber experts hack occupant’s platforms! As of today, a new feature is available in the chatbot @stop_russian_war_bot. This time you can fight together with us on the cyber front.” This chatbot marked the first state-sanctioned attempt to orchestrate overt counter-cyberconflict and to demonstrate the kind of hybrid resilience that would prove critical in the months to come.

One of the ITAU’s early defining characteristics was its paradoxically public nature. A notable advantage of cyberspace is its ability to give attackers anonymity; the ITAU inverted this advantage by making its cyber actions public. Similarly, while most government or government- adjacent defensive and offensive capabilities are shrouded in secrecy, the ITAU was created and is operated publicly. Over 311,000 people joined the ITAU of Ukraine on the social media platform Telegram within the first week of its creation, many with other full-time jobs during the day (Shead 2022). The ITAU’s overt operations and decentralization served both as a strength and a weakness in the Battle of Kyiv (Burgess 2022). Olexandr Bornyakov, Ukraine’s Deputy Minister of Digital Transformation and one of the government figures officially supporting the ITAU, noted “We don’t have a chain of command or any structure at all” (Bornyakov and Labott 2022). He clarified that his team gives general tasks to cyber combatants on Telegram but the specific implementation action is ultimately up to the group chat. Dmytro Budorin, Hacken’s chief executive officer, said in an interview: “It works very well. Everybody is communicating. Everybody is coordinating” (Cerulus 2022). Highlighting the military advantage of this decentralized strategy, Bornyakov also noted that Russia cannot disrupt or sabotage the group, as no one person holds decision-making power: it is a true collective effort of “digital soldiers” (Handa 2022).

Despite the group’s rapid growth and large number of participants, cohesion was facilitated by the presence of an overwhelming external threat. In an interview, one anonymous member of the ITAU stated: “At the start of the war, we had a problem of trust . . . But the situation we’re all in with the war has made all of us work together. We have become a hub for digital resistance here in Ukraine” (Temple-Raston and Powers 2022). As Agnes Venema of the Geneva Centre for Security Sector Governance stated, “this level of civic engagement [was] unprecedented” (Venema 2022; Houser 2022). The emergence of the ITAU was thus a direct consequence of this patriotic rally-around-the-flag effect, its existence signaling “a level of commitment across the country of Ukraine to resisting what the Russians are doing” (Burgess 2022; Pearson 2022a; Zitser 2022).

Cyberattacks against disinformation

From its conception, the ITAU made it clear that its goal was to support the Ukrainian government against Russia via both defensive measures like preventing attacks and debunking disinformation, as well as offensive measures like organizing cyberattacks against Russia. The ITAU's target list included Russian government websites, banks, and currency exchanges. This targeting aligned with Ukraine's goal of waging anti-disinformation campaigns by pushing back the Russian regime's narratives (RFE/RL 2021).

Although the invasion itself came as a surprise to most Russian domestic observers, sustained disinformation campaigns that started long before February 2022 had already primed Russian society and its army to accept the full-scale invasion as justified. In Russian online narratives, Ukrainians were characterized as brainwashed, their government a Western puppet without legitimacy (Thompson 2022). As Deputy Minister Bornyakov stated, disinformation was "really a core reason for this war because the Russians created a false picture of what's going on in Ukraine. And they convinced their citizens that Ukrainians are some sort of Nazis" (Bornyakov and Labott 2022). Debunking these false narratives was thus of key strategic importance to Ukraine's political authorities and the ITAU. On Telegram, ITAU members were instructed to fact-check and report any Russian disinformation they saw online. However, the ITAU had broader aims of harnessing the group's skills to hack into Russia's censored domestic networks and broadcast pro-Ukrainian text or footage (Pitrelli 2022). These sustained efforts to pierce Russia's digital defenses were the ITAU's key military and political contribution to Ukrainian victory in the Battle of Kyiv.

On 26 February, Russian troops reached the outskirts of Kyiv (Tsvetkova, 2025). Fighting ensued between the two armies and international media noted that Ukrainians were putting up a staunch defense, although many of the volunteers were young and untrained (Sky News 2022). Simultaneously, Ukrainians who were not on the physical frontlines were trying to bring the digital ones back towards Moscow.

Days after the invasion, the Russian government's official website, Kremlin.ru, was taken offline (Parsons 2022; Reuters 2022). The fact that Russia's primary official website was taken down held symbolic political significance, demonstrating that despite Russia's resources, its defenses could be penetrated even at the highest, most public levels of government. A few days later, as fighting around Kyiv continued, the ITAU successfully targeted the Moscow Stock Exchange's website and Sberbank, Russia's largest lender (T. Brewster 2022a). The exact hacking method and efficiency of both hacks by the ITAU have not been confirmed. However, the fact that Sberbank was offline on the afternoon of 28 February was verified by independent sources, including NetBlocks, an internet security and governance watchdog organization (Shead 2022).

In June 2022, Forbes Russia published an article discussing Sberbank's data and financial losses from cyberattacks since the start of the invasion. According to Sberbank Deputy Chairman of the Board Stanislav Kuznetsov, the data of 65 million Russians had been stolen by cyberattacks since the beginning of the "special military operation" in Ukraine. This included at least 13 million bank cards compromised, resulting in financial damages equating to 4.5 billion rubles, or around 72 million Canadian dollars (Tairov 2022).

Significantly, the ITAU posted about its successful Sberbank cyberattack during the first few days of the war with the caption “Sberbank Off!,” receiving thousands of positive Ukrainian reactions on Telegram. According to the same article, DDoS attacks blocked the services of 87 major Russian organizations for an hour or more since the invasion’s start. Kuznetsov further claimed the impact of cyber operations was felt most acutely in the financial sector, airlines, energy and oil and gas companies, logistics companies and internet vendors, as well as the media – all organizations the ITAU publicly announced targeting during and after the Battle of Kyiv. Indirectly confirming the ITAU’s successful strikes on these institutions, Russian foreign ministry spokeswoman Maria Zakharova told a domestic news outlet that Russian embassies were under cyberattack by “cyber terrorists from Ukraine” (Schechtman, Bing, and Pearson 2022).

The ITAU was not the only non-state actor to become involved with the Russia-Ukraine hybrid war. On the same day as the Stock Exchange and Sberbank hacks, the hacker group Anonymous successfully attacked Forbes Russia, taking down its website for a few hours and posting anti-governmental messages (Brewster 2022). However, the ITAU remained the only large-scale initiative, with the exclusive purpose of engaging in cyberconflict against Russia, and the only digital group directly sponsored and supported by Ukraine (Burgess 2022). Minister Fedorov thanked the ITAU for taking down Sberbank and the Stock Exchange on Facebook by posting “The mission has been accomplished! Thank you!” (Bornyakov 2022; T. Brewster 2022b). Deputy Minister Bornyakov noted that both the cyberattacks and the anti-disinformation campaigns stemmed from Ukraine’s existing IT talent and its people’s willingness to defend their country across all domains. Emphasizing the ITAU’s novelty in war, he stated “We are the first in the world to introduce this new warfare. And it’s powerful, yet simple at the same time” (Bornyakov and Labott 2022).

These early successes highlighted that in a hybrid war, control of information constituted an important part of building up resistance, maintaining domestic morale, and conveying a message of resilience to the outside world. The ITAU’s successful attacks reinforced their overall political mission in the Battle of Kyiv – to impose public costs on the invader and force them to divert resources away from the main arena of action.

Physical attacks on critical communications infrastructure were another element in the Battle of Kyiv. On 1 March 2022, a Russian missile struck Kyiv’s primary TV tower. Five civilians were killed and several wounded. Alongside the human losses, Ukraine’s government reported that a TV control room and a power substation were damaged, cutting off some Ukrainian channels from airing their information about crucial war developments (Welle 2022).

Following the attack, Ukraine’s Ministry of Defense tweeted warnings that some TV channels may stop signaling, although Ukraine’s engineers were working hard to restore back-up broadcasting. Furthermore, the Ministry stated that “The enemy can spread fakes in order to destabilize the situation. Know that Ukraine is fighting and persevering!”, directly linking the impact of physical attacks to higher risks of cyber exploitation (Defense of Ukraine 2022). The publication of Order 250 “On Additional Measures to Ensure Information Security of the Russian Federation” on 1 March by the Office of the President of the Russian Federation served as another official indication of cyberspace’s significance in the Battle of Kyiv (Decree of the President of the Russian Federation 2022).

Following this attack, questions were raised inside the government about whether the Ukrainian Army would seek retaliation (Beaumont, Boffey, and Russell 2022; D'Agata, Redman, and Ott 2022). However, despite popular sentiment, Ukraine was not prepared to impose revenge on Russia at the time. The Armed Forces and physical volunteer units were busy defending Kyiv from invasion. Counterstrikes into some captured territories, let alone into Russia directly, remained out of the question for physical combatants at the time. However, the ITAU's cyber character gave it more flexibility and opportunities to counter strike into Russian cyberspace.

As the ITAU demonstrated its abilities in the early days of the Battle of Kyiv, cyberwarfare experts raised questions about the effectiveness and ethics of these kinds of countermeasures (Schechtman, Bing, and Pearson 2022). While Russian infrastructure and financial services had been the primary target so far, the decentralized nature of the group meant some members could attempt to target Russian hospitals or other essential civilian infrastructure (Gill, 2025). Adding to this concern, ITAU coordinators, such as "Ted," made public statements that there are "no good or bad ways to fight during war" (BBC News, 2023). Although Ted's statement did not encapsulate the views of the entire ITAU, it reflected an attitude that some in the West considered dangerous. Western governments hesitated to express explicit support for the ITAU, likely due to the organization's operations' legal and ethical uncertainty. According to Michael E. van Lindingham, a former Russia analyst at the US Central Intelligence Agency, "Despite the United States government saying 'We're not allowing hacktivists to use American routers to do DDoS attacks on your state propaganda sites,' Russia is probably not going to believe that. . . . Russia uses cyber tools as an extension of state power. And Russian leaders mirror-image a lot. I think they'll perceive attacks from Anonymous or any Western collective as attacks that Western governments promote" (O'Neill, 2025).

During the Battle of Kyiv, Ukraine's government attempted to calm some of these Western worries, with Minister Fedorov stating, "Ukrainian cyber-experts have shown that despite such an invasion they operate ethically enough and do not cause unnecessary harm to any entities except Russian ones who are involved in the war and who have attacked our territory." Yet, alluding to the group's autonomous nature, a few seconds later he smiled and added, "I have never heard anything about those who are hacking Russia" (BBC News 2023; Fedorov 2022).

Despite some initial concerns, there were no reported ITAU attacks against Russian critical infrastructure (Duguin and Pavlova 2023; Schechtman, Bing, and; Pearson 2022a). Why not? The straightforward answer is that although Ukraine had technical experts, Russian critical systems were difficult to break into. Furthermore, planning large-scale attacks may take time, sometimes months or years of careful coordination. The ITAU's strength was its self-organized and decentralized nature, but this also meant that planning detailed, extensive attacks may have been difficult for the group. Although it would develop more precise, powerful cyberattacks as the war went on, its activities in the Battle of Kyiv were focused less on device damage and more on disruption through DDoS attacks (Houser 2022; Hunter, Douglas Albert, and Garrett 2021).

Whatever the opportunities presented by the ITAU, its amateur-by-design, decentralized nature also presented limits when it came to direct damage to Russian cyberspace. "The idea that you're going to grab this ragtag group of folk," said a former NSA hacker in a 2022 interview, "that they're going to somehow hack into the Kremlin's networks and

get valuable intelligence that's going to change the course, that's fantasy. DDoS and defensive is probably more important for Ukraine right now than offensive."¹⁰

Domestic morale and foreign perceptions

Despite its technical limits, the widespread support for the ITAU signaled a high level of participation among the civilian population. A fall 2022 survey by the Kyiv International Institute of Sociology (KIIS) found that 17% of Ukrainians had participated in either cyber-attacks or "information resistance" (i.e. counter-disinformation) campaigns (KIIS 2023). This percentage was higher, according to the report, among young and male respondents. In other words, a significant plurality of Ukrainians, especially among the younger generation, participated in the ITAU or partook other ITAU-like activities.

The popularity of this activity suggests broad societal recognition and endorsement of information resistance as both meaningful and effective. Given this level of voluntary participation, it is likely that Ukrainians perceived these kinds of activities as positively contributing to the war effort, thereby reinforcing morale. This widespread engagement, particularly among demographics influential in shaping national discourse, implies that the ITAU's initiatives resonated at home as acts of civic contribution, solidarity, and resilience.

Another source of evidence about the domestic impact of the ITAU is Ukrainian media coverage of the group and its activities. While a comprehensive media review of Ukrainian-language coverage is beyond the scope of this article, our perusal of representative newspaper reporting on the subject suggests Ukrainian media overwhelmingly portrays the group's activities in a positive light.

Union journalist Violetta Orlova, for example, emphasized that ITAU's success in digital warfare paralleled the broader physical resistance, writing that "the war has been ongoing not only on the front, but also in the information and digital spheres. The latter is being successfully managed by the IT Army of Ukraine" (Orlova 2022). *Facts* (2022) framed ITAU's operations as an "offensive cyber war," directly linking it to Ukraine's physical resistance and gathering significant public engagement (200,000 views), thus reinforcing a sense of national unity and active retaliation against Russian aggression. 2022 featured ITAU representatives discussing cyberattacks on Russian infrastructure. The widespread supportive comments from Ukrainians online which accompanied the program illustrated public recognition of ITAU's role in the war effort and cyberwarfare as a legitimate front in the conflict. As these examples demonstrate, the ITAU's actions were not only operationally significant but also symbolically powerful as a media narrative, reinforcing public confidence in Ukraine's ability to resist and adapt in an evolving conflict.

The morale-boosting qualities of the ITAU were also repeatedly noted by Western experts. Vasileios Karagiannopoulos, associate professor of cybersecurity at the University of Portsmouth, suggested the cyber-attacks may help "support defensive movements of the Ukrainian army." Yet the effects extended beyond cyberwarfare: "It also helps to symbolically generate an image of vulnerability that can impact on the morale of the opponents and respectively boost the morale of Ukrainian troops and citizens," he added (Manley 2024).

Expert analyses and scholarly commentary on the subject thus serve as another source of evidence of the ITAU's impact on shaping foreign perceptions of Ukrainian resistance.

Western think-tank experts and academics consistently highlight the ITAU as emblematic of Ukrainian innovation, social resilience, and effective asymmetric warfare against Russian information campaigns. As CEPA analyst David Kirichenko notes, since many countries cannot afford large dedicated cyber commands, Ukraine's easily deployable "volunteer IT army represents a potential blueprint" for cyber defense to be emulated by other states (Kirichenko 2023).

Foreign observers, including cybersecurity specialists, have also pointed to the ITAU as an important factor in resisting against Russian cyberattacks. "People from all corners of the world have joined the digital fight," wrote Elizabeth Braw in *Foreign Affairs* in 2022. "They have worked on projects ranging from disabling Russian government pages to building a website to combat Russian misinformation – and they have often succeeded" (Braw 2022).¹¹

A 2023 report by the Center for Strategic and International Studies (CSIS) noted that the IT Army "has quietly transformed from an ad-hoc force of volunteers into a tightly organized operation, with ongoing support from Ukrainian government officials, tens of thousands of international participants, and industry-leading tools" (Render-Katolik 2023).¹² As another Western analyst noted, the IT Army "is playing a crucial role in the war with Russia, launching disruptive cyber-attacks and data thefts against the Russian government and other high-profile targets" (Karagiannopoulos 2023). A June 2022 CyberPeace Institute report noted the ITAU and similar collectives "are committing cyberattacks at a rate and scale rarely seen before" (CyberPeace Institute 2022).¹³

A number of analysts have also praised ITAU's flexibility and recruitment strategy as a way to boost citizen participation. "This open recruitment strategy significantly lowered the barrier to entry for participating in DDoS attacks," notes cybersecurity expert Pascal Geenens (2024), "allowing individuals with minimal technical expertise to contribute to a collective cyber effort." Smith and Dean (2023, 103) refer to the IT Army as "a unique multinational, nonviolent resistance movement that leverages a creative structure to achieve operational impact." They go on to speculate that the ITAU "will likely inform cyber operational art in future conflicts."

These foreign observers frame the ITAU's efforts as not only tactically effective but also symbolically powerful, demonstrating Ukraine's resolve and ingenuity to an international audience. Their detailed accounts and analyses in Western publications thus validate the ITAU's broader symbolic success in projecting Ukraine's international image as resilient and resourceful in the face of aggression.

The comparison between Georgia in 2008 and Ukraine in 2022 provides further evidence of the ITAU's significance for both domestic morale and foreign perception of national resistance. In 2008, as Russia prepared to invade Georgia, it launched a coordinated cyber campaign alongside military action. These attacks – including DDoS and Cross-Site Scripting (XSS) assaults – targeted Georgian media and government websites. Some experts have identified this as the first documented case of cyber warfare directly accompanying a kinetic invasion (Shakarian 2011).

While these attacks did not disable Georgia's military response, they amplified the invasion's psychological impact (Beehner et al. 2018). By disrupting internet infrastructure, they prevented the Georgian state from immediately countering Russia's narrative, fostering uncertainty and undermining public confidence (Fraser 2022). In contrast, ITAU helped to ensure that Ukraine avoided this fate. By publicly declaring a campaign of

digital resilience, the group enabled Ukraine to shape its own information campaign, projecting an image of resistance rather than capitulation.

Beyond the battle of Kyiv: lessons of the resistance

In the months following Kyiv's successful military defense and political victory, Ukraine's government repeatedly stated that it had no plans to invade Russia and that its only mission was to retake conquered Ukrainian territories in the South and East (Guardian News 2022; Kauranen and Hunder 2023). However, even before the physical invasion of Kursk, Ukraine found ways to "attack to defend" – that is, going on offense while fending off an attack to elicit surprise and divert the enemy's resources. In one internationally noted instance, on 3 May 2023, a drone crashed into the Kremlin Senate building. The video of the Senate roof on fire was viewed and shared by millions (Kauranen and Hunder 2023). The visual of one of Russia's most important government buildings aflame was a powerful one, and the news of this accomplishment reverberated through Ukrainian social networks. Ukrainian officials denied their official involvement, emphasizing that attacking Russia was beyond Ukraine's goals of territorial defence (Buketov and Bushuev 2023). David Arakhamia, Head of the Servant of the People Parliamentary faction, wrote on Telegram that he thought sanctioned Russian elites were behind the attack and that "This is the first collective game of the 'offended club'". I hope – not the last (Arakhamia 2023). American intelligence organizations and officials, however, speculated that Ukraine's government was probably behind the attack (Barnes et al. 2023). This drone attack, and various similar ones following it, paralleled the ITAU's initial strategy in the Battle of Kyiv, whereby the attacks had more political meaning than military effectiveness. The attacks' purpose was to demonstrate to Russians, Ukrainians and the international community that Russia was indeed vulnerable, even if in symbolic ways, and the war was not one sided.

Minister Fedorov's smirking denial about any knowledge of the ITAU's activities leads to a curious point about cyberconflict's deniability in a hybrid war. One of cyberspace's most attractive elements is the relative anonymity it grants attackers (Jasper 2020; Schulze 2020). Although cyberattacks are often traceable, doing so requires immense effort and it is difficult to definitively identify one perpetrator, giving governments the flexibility to claim responsibility for some cyberattacks while plausibly denying others (Carlin and Graff 2018, 49).

The IT Army's actions during the Battle of Kyiv serve as a reminder that despite existing in different domains, both physical and cyber conflict have strong underlying psychological elements. While disinformation on its own cannot be classified as violence, it facilitated Russian aggression and shaped how Ukraine's resilience in the Battle of Kyiv was perceived, making it a crucial consideration in instances of hybrid warfare. Russia's initial disinformation set the stage for a physical confrontation and the ITAU's promotion of pro-Ukrainian narratives resulted in positive political perceptions of Ukraine's resilience (Levyatan 2022; Thompson 2022).

ITAU members have acknowledged that Russia's immense digital disinformation system is difficult to penetrate (Pitrelli 2022). Russia's preferred method for spreading disinformation has been to spread false, sometimes mutually inconsistent narratives with no regard for internal coherence. Public opinion surveys since the invasion, though

unreliable, suggest that at least some Russians have internalized myths about Ukraine – as did some foreign Western observers who were open to pro-Russian narratives (Sonnenfeld and Tian 2023). Since the start of the invasion, some Russian news outlets have been lampooned for their contradictory propaganda messages, such as that Ukrainians are both Nazis but also ethnic brothers. Yet a focus on such contradictions misses the point – Russian disinformation does not seek to create internal coherence, but only to create a sense of doubt, confusion, and ultimately epistemic nihilism that promotes apathy and acquiescence (Gunitsky 2015, 2020; Pomerantsev 2014).

Through successful cyberattacks, the ITAU was able to disrupt some of this Russian disinformation. As Minister Fedorov stated, “With the help of the IT Army, we managed to run a bunch of media campaigns to show the truth” (Bornyakov and Labott 2022). As Victor Zhora, the former deputy chief of Ukraine’s State Service of Special Communication, argued, the ITAU found success disrupting some Russian disinformation in the Battle of Kyiv by knocking systems offline and thus circumventing Russian domestic censorship (Schechner 2022). Yet while the ITAU’s actions in the Battle of Kyiv promoted Ukraine’s narrative domestically and internationally, it is difficult to discern the exact effect ITAU cyberattacks had on influencing domestic opinion within Russia itself.

However, some documented reactions to ITAU attacks suggest its cyberattacks successfully unnerved Russian citizens. On 3 March, an ITAU administrator announced the group’s priority targets in a Telegram chat. The Russian Central Bank was one such target. Two days later, the Russian newsletter *Ura* reported that “Due to hacker attacks that target providers, the work of the Fast Payment System may slow down in Russia” (Fedorovskikh and Zhabrikov, 2025). The comments under the article were indicative of the ITAU’s impact, with one user asking “Where are the praised Russian specialists!”, indicating surprise at Russia’s inability to defend its cyberspace. Another top comment complained “Now the Central Bank will block payment systems by itself and blame everything on the hackers!”, reflecting skepticism of the regime. And another noted: “A special operation is needed to identify the individuals involved and physically remove them from the action. All over the world, softly and quietly.” Thus at least some regular Russians perceived the cyberattacks as a serious concern.

When the full-scale invasion broke out, Russia saw large-scale protests, including in the capital (Taylor 2022). There was some hope that Russia’s conflict escalation could spark a tipping point of popular protest, leading to Russia’s regime overthrow. The ITAU’s cyberattack and anti-disinformation efforts supported these efforts, with Budorin stating that Ukrainian hackers have tried “to push people to take to the streets and to show that the Putin regime is about to fail” (Cerulus 2022).

The ITAU’s decentralized structure made it a difficult military target for Russian cyber operatives. Its spontaneous creation paralleled the emergence of Ukraine’s volunteer units at the start of the conflict. The ITAU’s vast membership and informal yet state-sponsored structure reflected the idea that Ukrainians with all skills could contribute to unified resistance against Russia. The group’s successful cyber strikes into Russian cyberspace disrupted state-produced disinformation but also fulfilled Ukrainians’ desire to impose costs on Russia for the escalation, even if the costs were mostly symbolic. By demonstrating Russia’s systematic vulnerabilities through successful, publicly confirmed cyberattacks, the ITAU boosted Ukrainian morale and international recognition of Ukraine as a resilient, sovereign state. This narrative was cemented when on 29 March Russia

announced it would “drastically reduce” its military assault on Kyiv and began withdrawing forces in the coming days (Hodge et al. 2022). Within three days, the Ukrainian government announced, “The whole Kyiv region is liberated from the invader” (Gardner, Bensemra, and Boumzar 2022). The war raged on, but the Battle of Kyiv had been won.

Cyberspace has blurred boundaries between peacetime agitation and wartime attacks. At the same time, hybrid war has also expanded the range of actors who may become involved in warfare. While violent physical actions remain at the core of any kinetic conflict, the rise of the ITAU demonstrates that cyber conflict is becoming increasingly crucial to framing these confrontations in the public mind, both to the warring parties and to the international community at large.

As the invasion demonstrated, online disinformation typically precedes physical action, priming both combatants and civilians for attacks. Once the physical war escalates into direct battles, disinformation both sustains false narratives that justified the incursion and sows disorganization within the battlefields. Cyberattacks on critical infrastructure and institutions, as well as disinformation before and about these actions, contribute to the fog of war that clouds immediate decision-making on the ground as well as domestic and international opinion. Cyberattacks on prominent national websites pierce disinformation hubs and attempt to inject alternative information into an otherwise limited discourse. Cyberattacks and disinformation thus operate in the same grey domain.

The group’s digital nature allows and encourages international participant involvement, raising ethical, political, and legal questions about the identity of cyber combatants. While this paper has highlighted the political benefits of solidarity through cyberconflict, it is unclear how engaging more civilians as cyber volunteers could impact the wartime society’s security and stability in the short and long term (Hakmeh and Naylor 2022). Furthermore, questions of digital combat involvement are particularly relevant when considering international cyber volunteers, located outside a war’s physical damage zones and being directly related to it by compassion, not passport or blood. As future hybrid wars will escalate, involving both traditional physical and contemporary cyber elements, it will be up to states to decide how to proceed with drawing the boundaries on their citizens’ cyber activities and conflict contributions.

As legal experts have argued, even if governments and IGOs were to draw up legislation to prohibit politically motivated digital volunteers such as ITAU, these would be nearly impossible to implement (Biggerstaff 2023). Even in peacetime, cyberattacks have posed consequential, costly problems to state and non-state actors. Hacker identification is difficult, and extradition and arrest are rare. These grey-area legalities may set a dangerous precedent for other governments, as having no legal frameworks in place could encourage more cyber volunteer groups to confront states or groups whose political missions they oppose (Soesanto 2023; Svantesson 2023).

The ITAU’s vast membership and successful attacks on Russia’s large institutions have raised worries about how cyberattacks could potentially ricochet back to Ukraine and beyond, thereby expanding the conflict (Burgess 2022). Novice hackers who sympathize with Ukraine’s cause from abroad may not know how to cover their tracks once they manage access to Russian systems – their actions make them vulnerable to becoming Russian targets (Schechner 2022). Civilians participating in the ITAU could also pose a Russian precedent for further conflict escalation, as it would validate Russia’s false claims that it is being attacked by the West and NATO (Soesanto

2023). So far, at least, the Kremlin has not used the involvement of outside online actors as a pretense for escalating the war. Yet worries of escalation, on physical and digital grounds, remain salient. With cyberspace a still-developing conflict zone, future wars are bound to create more opportunities for damage and escalation, whether accidental or deliberate.

Conclusion

The Battle of Kyiv was ultimately won on the physical battlefield. Yet the ITAU's cyber activities positively influenced the conflict's outcome and contributed to Ukraine's public relations successes by both preventing and launching cyberattacks. It did so by adopting a joint "attack to defend" cyberattack and anti-disinformation strategy that undermined Russian governmental and organizational online assets. As part of this approach, the ITAU disrupted Russian disinformation and inserted pro-Ukrainian messages into Russia's hacked information space where possible.

From the start, the ITAU used cyberattacks to divert Russian resources and attention away from direct military engagements. Yet perhaps more importantly, the ITAU's limited but public victories against symbolically important Russian sites like the Kremlin's official website, the Moscow Stock Exchange, and Sberbank also served to boost Ukrainian domestic morale. The ITAU thus served to channel Ukraine's desperation and anger – the attacks, originating from Kyiv-based virtual networks, reached where their physical soldiers could not. As Danylo Stolyarevskyi, an ITAU soldier who was turned away from Ukraine's physical army, stated, "It is a drop in the ocean, but you feel your small contribution to the common cause" (Lapatina 2022).

The ITAU's political contribution to the Battle of Kyiv also included shaping international narratives surrounding Ukraine's resistance and resilience. By openly targeting Russian cyber infrastructures and disinformation campaigns, the ITAU not only disrupted Russian operations and boosted domestic morale, but also influenced international perceptions about Ukraine's capacity to resist. Cyberspace, borderless by design, empowered the ITAU to contribute to a war over borders by emphasizing Ukrainians' connectivity with each other.

Unlike typical cyber warfare, the ITAU's operations were overt, often public-facing, and transparent, aiming to demoralize the adversary, shape public discourse, and solidify both domestic and international support. In that sense the ITAU reflects a broader transformation in cyber warfare – from covert operations focusing on damaging enemy resources, to public information campaigns aimed at disrupting propaganda and shaping global narratives. In the process, the ITAU has also served as a model for civilian engagement in national defense, democratizing participation in warfare to include non-traditional combatants. As William Done (2023) notes, the ITAU "offers a glimpse into the future of cyber warfare and could serve as a template for creating similar volunteer organizations in future conflicts."

The ITAU's cyber activities have played a key role in establishing Ukraine's hybrid resilience – its ability to withstand a sustained assault via both kinetic and digital attacks. The ITAU bolstered Ukraine's resilience by effectively combining online attacks and disinformation countermeasures to complement traditional military defenses. In doing so, it reflected and amplified Ukraine's emerging military and political ethos: to fight back.

Notes

1. On this point, see also Givens, Gorbachevsky, and Biernat (2023) and Lin (2022).
2. Kostyuk and Brantly (2022) argue that despite Western support and the transfer of cyber expertise, Ukraine's cyber defenses have faced operational and organizational constraints. Since traditional state-led cyber defense has limits in how it can be supported by partner nations, a group like the ITAU may have emerged as a way to circumvent these limits. The limits of formal interstate cooperation highlighted by Kostyuk and Brantly helped shape the emergence of the ITAU as a decentralized, volunteer-based force.
3. Brantly and Brantly (2024, 489) likewise discuss the "increasing resilience of Ukrainian cyber defenders." Willett (2022, 16) argues that "the biggest factor in Russia's cyber failure" has been "Ukraine's own cyber-security expertise."
4. Studies by Lewis (2022) and Willett (2022) likewise portray Ukraine's cyber defense as part of a broader "whole-of-society" effort.
5. Norman (2024) also describes the conflict as the "first conventional war to occur in an entirely connected information ecology."
6. As Braw (2022) argues, the lack of formal state control over these digital actors makes it difficult to regulate their actions, creating the potential for unintentional escalation or giving Russia a pretext for retaliation.
7. As Pfeifer and Schwab (2023) argue, the state versus non-state distinction becomes especially tenuous in modern conflicts, where non-state actors often perform state functions and states employ tactics associated with non-state actors.
8. In the early stages of the 2022 invasion, for instance, civilians filmed Russian military equipment and war crimes on their mobile devices and shared this intelligence with the Ukrainian Armed Forces through both official and unofficial social media channels (Lysenko 2024).
9. For instance, Hoffman, Neumeyer, and Jensen (2024) argue that a key element of NATO deterrence involves "establish[ing] resilience against adversaries' hybrid activities."
10. Quoted in Burgess (2022).
11. As Givens, Gorbachevsky, and Biernat (2023, 97) have noted: "Impressive Ukrainian cyber defense measures have blunted [Russian] attacks, contrary to predictions expressed by some Western intelligence services, technology firms, and scholars."
12. According to the report, the ITAU combines the "operational efficiency of a structured government agency and the versatility of a volunteer force. By integrating a state-led command structure, it has retained focus and purpose, and by allowing for independent operations, it has attracted many thousands of international volunteers" (Render-Katolik 2023).
13. "Our analysis underscores the significant role played by the IT Army among pro-Ukrainian threat actors," said a spokesperson from Institute" (quoted in Antoniuk 2024).

Disclosure statement

No potential conflict of interest was reported by the author(s).

References

- 24 Channel. 2022. "Zayava IT-Armii Ukraini pro kiberataki na Rosiiski TETs [Statement of the it Army of Ukraine on Cyberattacks Against Russian Thermal Power Plants]." *YouTube*. Accessed May 6, 2025. <https://www.youtube.com/watch?v=TkMiTwAEWco>.
- Antoniuk, Daryna. 2024. "How Ukraine's Volunteer Hackers Have Created a 'Coordinated Machine' Around Low-Level Attacks." *The Record*. April 4. Accessed April 22, 2025. <https://therecord.media/ukraine-volunteer-it-army-machine-low-level-attacks>.

- Arakhamia, David. 2023. "Bagato versii pro droni nad kremlem . . . [Many Versions About Drones Over the Kremlin . . .]." *Telegram*. Accessed April 22, 2025. https://t.me/s/David_Arakhamia.
- Barnes, Julian E., Adam Entous, Eric Schmitt, and Anton Troianovski. 2023. "Ukrainians Were Likely Behind Kremlin Drone Attack, U.S. Officials Say." *The New York Times*, May 24. Accessed April 22, 2025. <https://www.nytimes.com/2023/05/24/us/politics/ukraine-kremlin-drone-attack.html>.
- Bateman, Jon, Nick Beecroft, and Gavin Wilde. 2022. "What the Russian Invasion Reveals About the Future of Cyber Warfare." Carnegie Endowment for International Peace. December 19. Accessed April 22, 2025. <https://carnegieendowment.org/posts/2022/12/what-the-russian-invasion-reveals-about-the-future-of-cyber-warfare?lang=en>.
- BBC News. "How Ukraine and Russia are Rewriting the Rules of Cyber War." *YouTube*. Accessed April 22, 2023. <https://www.youtube.com/watch?v=zX9emwKYemE>.
- Beaumont, Peter, Daniel Boffey, and Graham Russell. 2022. "Ukraine's Zelenskyy Vows Revenge on Russian Forces After Fleeing Family Killed in Shelling of Irpin." *The Guardian*. March 7. Accessed April 22, 2025. <https://www.theguardian.com/world/2022/mar/07/ukraine-volodymyr-zelenskyy-vows-revenge-russia-forces-fleeing-family-civilians-killed-shelling-irpin-town>.
- Beehner, Lionel, Liam Collins, Steve Ferenzi, Robert Person, and Aaron Brantly. 2018. *Analyzing the Russian Way of War: Evidence from the 2008 Conflict with Georgia*. West Point, NY: Modern War Institute.
- Beliakova, Polina. 2022. "Volunteer Troops Can Be a Curse, Not a Blessing. But Ukraine May Be Figuring it Out." *The Washington Post*. February 27. Accessed April 22, 2025. <https://www.washingtonpost.com/politics/2022/02/27/volunteer-troops-can-be-curse-not-blessing-ukraine-may-be-figuring-it-out/>.
- Biggerstaff, William Casey. 2023. "The Status of Ukraine's 'IT Army' Under the Law of Armed Conflict." *Lieber Institute West Point*. Accessed April 22, 2025. <https://lieber.westpoint.edu/status-ukraines-it-army-law-armed-conflict/>.
- Bornyakov, Oleksandr. 2022. "The Mission Has Been Accomplished! Thank You!" Facebook.
- Bornyakov, Oleksandr, and Elise Labott. 2022. "We are the First in the World to Introduce This New Warfare: Ukraine's Digital Battle Against Russia." *Politico*, March 8 social-media-00014880. Accessed April 22, 2025. <https://www.politico.com/news/magazine/2022/03/08/ukraine-digital-minister-crypto-cyber->.
- Brantly, Aaron F., and Nataliya D. Brantly. 2024. "The Bitskrieg That was and wasn't: The Military and Intelligence Implications of Cyber Operations During Russia's War on Ukraine." *Intelligence and National Security* 39 (3): 475–495. <https://doi.org/10.1080/02684527.2024.2321693>.
- Braw, Elisabeth. 2022. "Ukraine's Digital Fight Goes Global." *Foreign Affairs*, May 2. Accessed April 22, 2025. <https://www.foreignaffairs.com/ukraine/ukraines-digital-fight-goes-global>.
- Brewster. 2002. "Russian Media Websites Hacked, Anonymous Claims Responsibility." *RadioFreeEurope/Radioliberty*. Accessed April 22, 2025. <https://www.rferl.org/a/russia-websites-hacked-anonymous/31728186.html>.
- Brewster, Thomas. 2022a. "If Kyiv Falls, We Keep Hacking Putin': On the Cyber Front Line in Ukraine." *Forbes*. February 25. Accessed April 22, 2025. <https://www.forbes.com/sites/thomasbrewster/2022/02/25/if-kyiv-falls-we-keep-hacking-putin-on-the-cyber-frontline-in-ukraine/?sh=9199b935a6e2>.
- Brewster, Thomas. 2022b. "Moscow Exchange, Sberbank Websites Knocked Offline—Was Ukraine's Cyber Army Responsible?" *Forbes*. February 28. Accessed April 22, 2025. <https://www.forbes.com/sites/thomasbrewster/2022/02/28/moscow-exchange-and-sberbank-websites-knocked-offline-was-ukraines-cyber-army-responsible/?sh=25a5802b77ca>.
- Buketov, Kirill, and Mikhail Bushuev. 2023. "Udar bespilotnikami po Kremlyu: Instsenirovka ili net? [Drone Strike on the Kremlin: Staged or Real?]." *DW*, inscenirovka-ili-net/a-65514579. Accessed April 22, 2025. <https://www.dw.com/ru/udar-bespilotnikami-po-kremlyu->.
- Burgess, Matt. 2022. "Ukraine's Volunteer 'IT Army' is Hacking in Uncharted Territory." *Wired*. February 27. Accessed April 22, 2025. <https://www.wired.com/story/ukraine-it-army-russia-war-cyberattacks-ddos/>.
- Carlin, John P., and Garrett M. Graff. 2018. *Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat*. New York: PublicAffairs.

- Carvin, Stephanie. 2022. "Is Ukraine the Cyberwar That Wasn't?" *Centre for International Governance Innovation*. Accessed April 22, 2025. <https://www.cigionline.org/articles/is-ukraine-the-cyberwar-that-wasnt/>.
- Casey, Adam, and Seva Gunitsky. 2022. "The Bully in the Bubble." *Foreign Affairs*. February 4. Accessed May 5, 2025. <https://www.foreignaffairs.com/articles/russian-federation/2022-02-04/bully-bubble>.
- Cerulus, Laurens. 2022. "Kyiv's Hackers Seize Their Wartime Moment." *Politico*. March 10. Accessed April 22, 2025. <https://www.politico.eu/article/kyiv-cyber-firm-state-backed-hacking-group/>.
- Check Point Research Team. 2022. "Cyber Attack Trends in the Midst of Warfare." *Check Point Blog*. Accessed April 22, 2025. <https://blog.checkpoint.com/security/196-increase-in-cyber-attacks-on-ukraines-government-and-military-sector/>.
- CyberPeace Institute. 2022. "Ukraine Conflict: Cyberattacks—Frequently Asked Questions." *CyberPeace Institute*. Accessed April 22, 2025. <https://cyberpeaceinstitute.org/news/ukraine-conflict-cyberattacks-frequently-asked-questions/>.
- D'Agata, Charlie, Justine Redman, and Haley Ott. 2022. "Kyiv Residents Say They're 'Not Ready to Give Up' as They're Given Guns to Help Defend Their City." *CBS News*. February 25. Accessed May 6, 2025. <https://www.cbsnews.com/news/russia-ukraine-invasion-kyiv-civilians-volunteer-get-guns-help-defend-city/>.
- Decree of the President of the Russian Federation. 2022. "Decree of the President of the Russian Federation from 01.05.2022 № 250 · Official Publication of Legal Acts." *Official Publication of Legal Acts*. March 1. Accessed April 22, 2025. <http://publication.pravo.gov.ru/Document/View/0001202205010023>.
- Defense of Ukraine. 2022. "UVAGA. Popadaniya v aparatnu movnika na televizhi. Yakiis' chas, kanali ne budut' pratsyuvati ... [WARNING. Getting into the Broadcaster's Hardware on the TV Tower. For a While, the Channels Will Not Work ...]." *Twitter*. Accessed April 22, 2025. <https://twitter.com/DefenceU/status/1498685345197703175>.
- Done, William D. 2023. "The Information Technology Army of Ukraine and Cyber Warfare Doctrine." *Journal of Strategic Security* 16 (4): 15–33.
- Duguin, Stéphane, and Pavlina Pavlova. 2023. "The Role of Cyber in the Russian War Against Ukraine: Its Impact and the Consequences for the Future of Armed Conflict." *European Parliament*. Accessed April 22, 2025. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI\(2023\)702594_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf).
- ESET. 2022. "ESET Research: Ukraine Hit by Destructive Attacks Before and During the Russian Invasion with Hermeticwiper and Isaacwiper." *ESET Press Release*. March 1. Accessed April 22, 2025. <https://www.eset.com/int/about/newsroom/press-releases/research/eset-research-ukraine-hit-by-destructive-attacks-before-and-during-the-russian-invasion-with-hermet/>.
- Facts, I. C. T. V. 2022. "Cyberwar Against Russia: How Ukraine and the World are Winning in the Information Space." *YouTube*. Accessed April 22, 2025. <https://www.youtube.com/watch?v=S9gbtJ7I754>.
- Fedorov, Mykhailo. 2022. "We are Creating an it Army. We Need Digital Talents. All Operational Tasks Will Be Given Here: Htps://T.Me/Itarmyofurraine. There Will Be Tasks for Everyone. We Continue to Fight on the Cyber Front. The First Task is on the Channel for Cyber Specialists." *Twitter*. Accessed April 22, 2025. <https://twitter.com/FedorovMykhailo/status/1497642156076511233>.
- Fedorovskikh, Marina, and Vladimir Zhabrikov. "Central Bank: Hacker Attacks Slow Down the Russian Faster Payments System." *RIA URA.RU*. March 5. Accessed April 22, 2025. <https://ura.news/news/1052536905>.
- Fix, Liana, and Michael Kimmage. 2022. "What if Russia Wins? A Kremlin-Controlled Ukraine Would Transform Europe." *Foreign Affairs*. February 18. Accessed April 22, 2025. <https://www.foreignaffairs.com/articles/ukraine/2022-02-18/what-if-russia-wins>.
- Ford, Matthew. 2024. "From Innovation to Participation: Connectivity and the Conduct of Contemporary Warfare." *International Affairs* 100 (4): 1531–1549. <https://doi.org/10.1093/ia/iaae061>.
- Fraser, Cameron. 2022. "How Russian Disinformation Tactics Were Utilised in the Context of the 2008 5-Day War." *Institute for Development of Freedom of Information*. Accessed April 22, 2025.

- https://idfi.ge/en/how_russian_disinformation_tactics_were_utilised_in_the_context_of_the_2008_5_day_war.
- Garber, Megan. 2022. "The Grim Stagecraft of Zelensky's Selfie Videos." *The Atlantic*. February. Accessed April 22, 2025. <https://www.theatlantic.com/culture/archive/2022/02/zelensky-ukraine-president-selfie-video-kyiv/622949/>.
- Gardner, Simon, Zohra Bensemra, and Abdelaziz Boumzar. 2022. "Ukraine Claims Control over Kyiv Region as Russia Looks East." *National Post*. April 3. Accessed April 22, 2025. <https://nationalpost.com/pmnn/news-pmn/ukraine-claims-control-over-kyiv-region-as-russia-looks-east-5>.
- Geenens, Pascal. 2024. "The Democratization of DDoS Attacks: Insights from the IT Army of Ukraine's Cyber Campaign." *Radware Blog*. February 21. Accessed April 22, 2025. <https://www.radware.com/blog/ddos-protection/the-democratization-of-ddos-attacks-insights-from-the-it-army-of-ukraines-cyber-campaign/>.
- Gill, Jaspreet. "Why Ukraine Recruiting Amateur 'IT Army' Could Backfire." *Breaking Defense*. March. Accessed April 22, 2025. <https://breakingdefense.com/2022/03/why-ukraine-recruiting-amateur-it-army-could-backfire/>.
- Givens, Austen D., Max Gorbachevsky, and Anita C. Biernat. 2023. "How Putin's Cyberwar Failed in Ukraine." *Journal of Strategic Security* 16 (2): 96–121. <https://doi.org/10.5038/1944-0472.16.2.2099>.
- Grzegorzewski, Mark, Margaret Smith, and Barnett Koven. 2023. "Civil Cyber Defense—A New Model for Cyber Civic Engagement." *The Cyber Defense Review* 8 (3): 51–66.
- Guardian News. 2022. "'We Will Defend Ourselves', Says Ukrainian President Volodymyr Zelenskiy." *YouTube*. Accessed April 22, 2025. <https://www.youtube.com/watch?v=prfaWHQoxVg>.
- Gunitsky, Seva. 2015. "Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Resilience." *Perspectives on Politics* 13 (1): 42–54. <https://doi.org/10.1017/S1537592714003120>.
- Gunitsky, Seva. 2020. "The Great Online Convergence: Digital Authoritarianism Comes to Democracies." *War on the Rocks*. February 19. Accessed May 6, 2025. <https://warontherocks.com/2020/02/the-great-online-convergence-digital-authoritarianism-comes-to-democracies/>.
- Hakmeh, Joyce, and Esther Naylor. 2022. "How the Tech Community Has Rallied to Ukraine's Cyber-Defence." *The Guardian*. March 7. Accessed April 22, 2025. <https://www.theguardian.com/commentisfree/2022/mar/07/tech-community-rallied-ukraine-cyber-defence-eu-nato>.
- Handa, Robert. 2022. "'We are Digital Soldiers': Silicon Valley Executive Helps Ukraine Using Tech Knowledge." *NBC Bay Area*. March 7. Accessed April 22, 2025. <https://www.nbcbayarea.com/news/local/south-bay/we-are-digital-soldiers-silicon-valley-executive-helps-ukraine-using-tech-knowledge/2831362/>.
- Hodge, Nathan, Daria Markina, Tim Lister, Niamh Kennedy, and Lindsay Isaac. 2022. "Russia Says it Will Reduce Military Operations Around Kyiv Following Talks with Ukraine." *CNN*. March 29. Accessed April 22, 2025. <https://edition.cnn.com/2022/03/29/europe/russia-reduce-assault-kyiv-plan-intl/index.html>.
- Hoffman, Frank, Matt Neumeyer, and Benjamin Jensen. 2024. "The Future of Hybrid Warfare." *Center for Strategic and International Studies*. July 8. Accessed April 21, 2025. <https://www.csis.org/analysis/future-hybrid-warfare>.
- Houser, Kristin. 2022. "International Army of Hackers Joins Ukraine's Cyberwar." *Freethink*. March 16. Accessed April 22, 2025. <https://www.freethink.com/hard-tech/ukraine-it-army>.
- Hunter, Lance Y., Craig Douglas Albert, and Eric Garrett. 2021. "Factors That Motivate State-Sponsored Cyberattacks." *The Cyber Defense Review* 6 (2): 111–128.
- Jasper, Scott. 2020. *Russian Cyber Operations: Coding the Boundaries of Conflict*. Washington, DC: Georgetown University Press.
- Karagiannopoulos, Vasileios. 2023. "Ukraine's IT Army is a World First—Here's Why it is an Important Part of the War." *The Conversation*. October 25. Accessed April 22, 2025. <https://theconversation.com/ukraines-it-army-is-a-world-first-heres-why-it-is-an-important-part-of-the-war-212745>.
- Karmanau, Yuras. 2022. *Ukraine Says Russia Behind Cyberattack in 'Hybrid War' Move*. PBS. <https://www.pbs.org/newshour/world/ukraine-says-russia-behind-cyberattack-in-hybrid-war-move>.
- Kaska, Kadri, Anna-Maria Osula, and Jan Stinissen. 2013. *The Cyber Defence Unit of the Estonian Defence League: Legal, Policy and Organisational Analysis*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

- Kauranen, Anne, and Max Hunder. 2023. "Zelenskiy Denies Attacking Moscow, Vows to Start Counteroffensive." *Reuters*. May 3. Accessed April 22, 2025. <https://www.reuters.com/world/europe/ukraines-zelenskiy-finland-meet-with-nordic-leaders-2023-05-03/>.
- KIIS (Kyiv International Institute of Sociology). 2023. "'SCORE-Inspired Holistic Assessment of Resilience of Population (SHARP): Wave 2 Findings.'" December 6, 2023. https://www.kiis.com.ua/materials/news/20240126_n/PRE_SHARP2_Wave2_Initial_analysis_06.12.2023_ENG.pdf.
- Kirichenko, David. 2023. "Ukraine's Volunteer Army Confronts Tech, Legal Challenges." *Center for European Policy Analysis*. November 27. <https://cepa.org/article/ukraine-volunteer-it-army-confronts-tech-legal-challenges/>.
- Kostyuk, Nadia. 2015. *Ukraine: A Cyber Safe Haven.* *Cyber War in Perspective: Russian Aggression Against Ukraine*. Tallinn: NATO CCD COE Publications.
- Kostyuk, Nadiya, and Aaron Brantly. 2022. "War in the Borderland Through Cyberspace: Limits of Defending Ukraine Through Interstate Cooperation." *Contemporary Security Policy* 43 (3): 498–515. <https://doi.org/10.1080/13523260.2022.2093587>.
- Kostyuk, Nadiya, and Erik Gartzke. 2022. "Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine." *Texas National Security Review* 3 (Summer): 113–126.
- Lapatina, Anastasiia. 2022. "Putin Picked the Wrong Country to Mess with." *The New York Times*, March 5. Accessed April 22, 2025. <https://www.nytimes.com/2022/03/05/opinion/ukraine-russia-invasion.html>.
- Levyatan, Yaniv. 2022. "The First Tiktok War." *The Jerusalem Strategic Tribune*, April 7. Accessed April 22, 2025. <https://jstribune.com/levyatan-the-first-tiktok-war/>.
- Lewis, James A. 2022. "Cyber War and Ukraine." Center for Strategic and International Studies (CSIS), June 16. Accessed April 22, 2025. <https://www.csis.org/analysis/cyber-war-and-ukraine>.
- Lin, Herbert. 2022. "Russian Cyber Operations in the Invasion of Ukraine." *The Cyber Defense Review* 7 (4): 31–46.
- Lysenko, Anna. 2024. *Eyes Everywhere, All Against Enemies: Analyzing Non-Governmental Open-Source Intelligence's (NGOSINT) Value for Ukraine in the 2022 Russo-Ukrainian War (RUW)*, Ottawa, Canada. Canadian Association for Security and Intelligence Studies.
- Manley, Cameron. 2024. "Ukraine's Army is a 'World First' in Cyberwarfare, but It's a Gamble." *Business Insider*. July 27. Accessed April 22, 2025. <https://www.businessinsider.com/ukraines-it-army-world-first-cyberwarfare-but-a-gamble-2024-7>.
- Mathews, Lee. 2022. "Viasat Reveals How Russian Hackers Knocked Thousands of Ukrainians Offline." *Forbes*. March 31. Accessed April 30, 2025. <https://www.forbes.com/sites/leemathews/2022/03/31/viasat-reveals-how-russian-hackers-knocked-thousands-of-ukrainians-offline/?sh=13205a1660d6>.
- Merrin, William. 2018. *Digital War: A Critical Introduction*. London: Routledge.
- Miller, Maggie. 2022a. "Despite Years of Preparation, Ukraine's Electric Grid Still an Easy Target for Russian Hackers." *Politico*. Accessed April 30, 2025. <https://www.politico.com/news/2022/02/19/despite-years-of-preparation-ukraines-electric-grid-still-far-from-ready-for-russian-hackers-00010373>.
- Miller, Maggie. 2022b. "The World Holds Its Breath for Putin's Cyberwar." *Politico*. Accessed April 30, 2025. <https://www.politico.com/news/2022/03/23/russia-ukraine-cyberwar-putin-00019440>.
- Mueller, Grace B., Benjamin Jensen, Brandon Valeriano, Ryan C. Maness, and Jose M. Macias. 2023. "Cyber Operations During the Russo-Ukrainian War: From Strange Patterns to Alternative Futures." *Center for Strategic and International Studies (CSIS)*. July 18. Accessed April 30, 2025. <https://www.csis.org/podcasts/audio-briefs/cyber-operations-during-russo-ukrainian-war-audio-brief-ben-jensen>.
- Nagl, John. 2022. "Will Ukraine Be Afghanistan All Over Again for Russia?" *Foreign Policy*. February 22. Accessed April 30, 2025. <https://foreignpolicy.com/2022/02/22/ukraine-russia-afghanistan-defeat-insurgency/>.
- Nakashima, Ellen, and Alex Horton. 2022. "Russian Hackers Have Probably Penetrated Critical Ukraine Computer Networks, U.S. Says." *The Washington Post*, February 15. Accessed April 30, 2025. <https://www.washingtonpost.com/national-security/2022/02/15/russia-ukraine-cyber-attacks/>.

- Neuman, Scott. "Ukraine is Hit by a Massive Cyberattack That Targeted Government Websites." *NPR*. January 14. Accessed April 30, 2025. <https://www.npr.org/2022/01/14/1073001754/ukraine-cyber-attack-government-websites-russia>.
- Norman, Jethro. 2024. "War Volunteers in the Digital Age: How New Technologies Transform Conflict Dynamics." *Policy Brief*, Danish Institute for International Studies. July 1.
- O'Neill, Patrick Howell. "The Propaganda War Has Eclipsed Cyberwar in Ukraine." *MIT Technology Review*. May 11. Accessed April 30, 2025. <https://www.technologyreview.com/2022/03/02/1046646/the-propaganda-war-has-eclipsed-cyberwar-in-ukraine/>.
- Orlova, Violetta. 2022. "Ukraine's IT Army: What it Does and What Victories it Has Already Achieved." *Unian*. Accessed April 30, 2025. <https://www.unian.ua/techno/communications/it-armiya-ukrajini-chim-vona-zaymayetsya-ta-yaki-peremogi-vzhe-na-jiji-rahunku-11803026.html>. (in Ukrainian).
- Parsons, Robert. 2022. "'Our Fighting Spirit is 120 Percent': Ukrainian Troops Determined as Russian Forces Approach Kyiv." *France 24*. Accessed April 30, 2025. <https://www.france24.com/en/europe/20220227-our-fighting-spirit-is-120-percent-ukrainian-troops-determined-as-russian-forces-approach-kyiv>.
- Pearson, James. 2022a. "Ukraine Launches 'IT Army,' Takes Aim at Russian Cyberspace." *Reuters*. February 26. Accessed April 30, 2025. <https://www.reuters.com/world/europe/ukraine-launches-it-army-takes-aim-russian-cyberspace-2022-02-26/>.
- Pfeifer, Hanna, and Regine Schwab. 2023. "Re-Examining the State/non-State Binary in the Study of (Civil) War." *Civil Wars* 25 (2–3): 428–451. <https://doi.org/10.1080/13698249.2023.2254654>.
- Pitrelli, Monica. 2022. "'For the First Time in History Anyone Can Join a War'." *CNBC*, March 14. Accessed April 30, 2025. <https://www.cnbc.com/2022/03/14/volunteers-sign-up-to-help-in-cyberwars-between-russia-and-ukraine.html>.
- Pomerantsev, Peter. 2014. "Russia and the Menace of Unreality." *The Atlantic*. September 9. Accessed May 6, 2025. <https://www.theatlantic.com/international/archive/2014/09/russia-putin-revolutionizing-information-warfare/379880/>.
- Render-Katolik, Aiden. 2023. "The IT Army of Ukraine." *Center for Strategic and International Studies*. August 15. Accessed April 30, 2025. <https://www.csis.org/blogs/strategic-technologies-blog/it-army-ukraine>.
- Reuters. 2022. "Official Kremlin Website Down Amid War in Ukraine." *Reuters*. February 26. Accessed April 30, 2025. <https://www.reuters.com/world/europe/official-kremlin-website-down-amid-war-ukraine-2022-02-26/>.
- RFE/RL. 2021. "Ukraine Says Russia Ignoring Calls for Dialogue Amid Rising Tensions." *RadioFreeEurope/Radioliberty*. April 12. Accessed April 30, 2025. <https://www.rferl.org/a/ukraine-russia-ignoring-calls-for-dialogue/31199468.html>.
- Schechner, Sam. 2022. "Ukraine's 'IT Army' Has Hundreds of Thousands of Hackers, Kyiv Says." *The Wall Street Journal*. March 4. <https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-03-04/card/ukraine-s-it-army-has-hundreds-of-thousands-of-hackers-kyiv-says-RfpGa5zmLtavrot27OWX>.
- Schectman, Joel, and Christopher Bing. 2022. "Ukraine Calls on Hacker Underground to Defend Against Russia." *Reuters*, February 24. Accessed April 30, 2025. <https://www.reuters.com/world/exclusive-ukraine-calls-hacker-underground-defend-against-russia-2022-02-24/>.
- Schectman, Joel, Christopher Bing, and James Pearson. 2022. "Ukrainian Cyber Resistance Group Targets Russian Power Grid, Railways." *Reuters*, March 1. Accessed April 30, 2025. <https://www.reuters.com/technology/ukrainian-cyber-resistance-group-targets-russian-power-grid-railways-2022-03-01/>.
- Schulze, Matthias. 2020. "Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations." *2020 12th International Conference on Cyber Conflict (CyCon)*, Tallinn, Estonia: 183–197. Accessed April 30, 2025. <https://ccdcoc.org/library/publications/12th-international-conference-on-cyber-conflict-20-20-vision-the-next-decade-proceedings-2020/>.
- Schulze, Matthias, and Mika Kerttunen. 2023. "Cyber Operations in Russia's War Against Ukraine: Uses, Limitations, and Lessons Learned so Far." In *SWP Comment*. 2023/C 23, April 17. <https://www.swp-berlin.org/10.18449/2023C23/>.

- Security Service of Ukraine. 2022a. "CYBER FRONT is NOW OPEN! Help Ukrainian Cyber Experts Hack Occupant's Platforms! As of Today, a New Feature is Available in the Chatbot @stop_russian_war_bot. This Time You Can Fight Together with Us on the Cyber Front." *Twitter*. February 28. Accessed April 30, 2025. <https://twitter.com/ServiceSsu/status/1498261578969497601>.
- Security Service of Ukraine. 2022b. "SBU posiliuie kiberzakhyst stratehichnykh ob'ektiv i stvoriuie dlia toho 'hariachu' elektronnu adresu [The SBU Strengthens the Cyber Protection of Strategic Objects and Creates a "Hot" Email Address for This Purpose]." *Government of Ukraine*. Accessed April 30, 2025. <https://ssu.gov.ua/novyny/sbu-posyliuie-kiberzakhyst-stratehichnykh-obiektiv-i-stvoriuie-dlia-tsoho-hariachu-elektronnu-adresu>.
- Shakarian, Paulo. 2011. "The 2008 Russian Cyber-Campaign Against Georgia." *Military Review* 91 (6): 61.
- Shead, Sam. 2022. "'We Want Them to Go to the Stone Age': Ukrainian Coders are Splitting Their Time Between Work and Cyber Warfare." *CNBC*. March 23. Accessed April 30, 2025. <https://www.cnbc.com/2022/03/23/ukrainian-coders-splitting-their-time-between-day-job-and-cyberwar.html>.
- Shopina, Iryna, Dmytro Khomiakov, Nadiia Khrystynchenko, Serhii Zhukov, and Dmytro Shpenov. 2020. "Cybersecurity: Legal and Organizational Support in Leading Countries, NATO and EU Standards." *Journal of Security and Sustainability Issues* 9 (3): 977–992. [https://doi.org/10.9770/jssi.2020.9.3\(22\)](https://doi.org/10.9770/jssi.2020.9.3(22)).
- Singer, P. W., and T. Brooking. Emerson. 2018. *LikeWar: The Weaponization of Social Media*. Boston: Houghton Mifflin Harcourt.
- Sky News. 2022. "Ukrainian Soldier Guarding Kyiv Has Only Fired 16 Rounds in His Life." *YouTube*. Accessed April 30, 2025. <https://www.youtube.com/watch?v=SB1cxl3qDA>.
- Smith, Margaret, and Thomas Dean. 2023. "The Irregulars: Third-Party Cyber Actors and Digital Resistance Movements in the Ukraine Conflict." *15th International Conference on Cyber Conflict: Meeting Reality (CyCon)*, Tallinn, Estonia: 103–119. Accessed April 30, 2025. <https://ccdcoe.org/library/publications/15th-international-conference-on-cyber-conflict-meeting-reality/>.
- Soesanto, Stefan. 2022. "IT Army of Ukraine: 'Structure, Tasking, and Ecosystem.'" *CSS Cyberdefense Reports*. Accessed April 30, 2025. <https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/552293/Cyber-Reports-2022-06-IT-Army-of-Ukraine.pdf?sequence=2&isAllowed=y>.
- Soesanto, Stefan. 2023. "Ukraine's IT Army." *Survival* 65 (3): 93–106. <https://doi.org/10.1080/00396338.2023.2218701>.
- Sonnenfeld, Jeffrey, and Steven Tian. 2023. "Putin's Ongoing Disinformation War in the Western Media." *Time*. May 1. Accessed April 30, 2025. <https://time.com/6276130/putins-disinformation-war-western-media/>.
- Stepaniuk, Nataliia. 2022. "Wartime Civilian Mobilization: Demographic Profile, Motivations, and Pathways to Volunteer Engagement Amidst the Donbas War in Ukraine." *Nationalities Papers*: 1–18. <https://doi.org/10.1017/nps.2021.82>.
- Svantesson, Dan Jerker B. 2023. "Ukraine is Recruiting an 'IT Army' of Cyber Warriors. Here's How Australia Could Make it Legal to Join." *The Conversation*. March 6. Accessed April 30, 2025. <https://theconversation.com/ukraine-is-recruiting-an-it-army-of-cyber-warriors-heres-how->
- Tairov, Rinat. 2022. "Sberbank Claims Data Exfiltration of 65 Million Russians Since February 24." *Forbes.ru*. June 16. Accessed April 30, 2025. <https://www.forbes.ru/tekhnologii/468879-sberbank-zaavil-ob-utecke-dannyh-65-mln-rossian-s-24-fevrala>. (in Russian).
- Taylor, Alan. 2022. "Anti-War Protests in Russia." *The Atlantic*. February 24. Accessed April 30, 2025. <https://www.theatlantic.com/photo/2022/02/photos-anti-war-protests-russia/622914/>.
- Temple-Raston, Dina, and Sean Powers. 2022. "Inside the it Army of Ukraine, 'A Hub for Digital Resistance'." *The Click Here Podcast*, September 15. Accessed April 30, 2025. <https://theworld.org/stories/2022/09/15/inside-it-army-ukraine-hub-digital-resistance>.
- Thompson, Stuart A. 2022. "4 Falsehoods Russians are Told About the War." *The New York Times*, March 10. <https://www.nytimes.com/2022/03/10/technology/disinformation-russia-ukraine.html>.
- TSN. 2022. "Boroniti ukrayinski viyska zapisalis 37 tisyach ocib [37,000 People Signed Up to Defend Ukraine in the Teroborona Ranks]." *TSN.ua*. Accessed April 30, 2025. <https://tsn.ua/ato/boroniti-ukrayinski-viyska-zapisalis-37-tisyach-ukrayinciv-1989982.html>.

- Tsvetkova, Maria. 2025. "Fighting Reaches the Outskirts of Kyiv." *Reuters*, February 25. April 30. <https://www.reuters.com/world/europe/ukraines-president-stays-put-russian-invaders-advance-2022-02-25/>.
- Venema, Agnes. 2022. *This Level of Civic Engagement was Unprecedented*. Geneva: Geneva Centre for Security Sector Governance.
- Voo, Julia, Irfan Hemani, Simon Jones, Winnona DeSombre, Dan Cassidy, and Anina Schwarzenbach. 2020. "National Cyber Power Index 2020." *Harvard Kennedy School. Belfer Center for Science and International Affairs*. Accessed April 30, 2025. https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf.
- Welle, Deutsche. 2022. "Ukraine: Kyiv TV Tower Hit, 5 Reported Dead." *DW*. March 1. Accessed April 22, 2025. <https://www.dw.com/en/ukraine-says-5-dead-after-russian-missile-hit-kyiv-tv-tower-as-it-happened/a-60954234>.
- Wheat, Treston, and David Kirichenko. 2024. "Democratization of Irregular Warfare: Emerging Technology and the Russo-Ukrainian War." *Military Review* 104 (6): 45–54.
- Willett, Marcus. 2022. "The Cyber Dimension of the Russia–Ukraine War." *Survival* 64 (5): 7–26. <https://doi.org/10.1080/00396338.2022.2126193>.
- Wolff, Josephine. 2022. "Why Russia Hasn't Launched Major Cyber Attacks." *Time*. March 2. Accessed April 30, 2025. <https://time.com/6153902/russia-major-cyber-attacks-invasion-ukraine/>.
- Zitser, Joshua. 2022. "Video Reportedly Shows Ukrainian Men Helping Themselves to Guns on a Kyiv Street After All 18–60 Years Were Urged to Take Up Arms and Fight the Russian Invasion." *Business Insider*. Accessed April 30, 2025. <https://www.businessinsider.com/video-ukrainian-men-help-themselves-to-guns-in-kyiv-as-russia-attacks-2022-2>.