Policy Perspectives
Vol. 10/3, May 2022

CSS
ETH Zürich

Goodbye Cyberwar: Ukraine as Reality Check

Evidence from Ukraine shows that cyber operations are either too slow, too weak, or too volatile to provide significant strategic value in hybrid conflict and war.

By Lennart Maschmeyer and Myriam Dunn Cavelty

Before Russia's invasion of Ukraine, a series of experts predicted cyberwar: the massive use of Russian offensive cyber capabilities to "shock and awe" Ukraine's defenses and undermine their will to fight. Some even suggested Russia need not invade because it could achieve the same outcomes by going to cyberwar.

When that did not happen, the same experts predicted that Russia would still use offensive cyber capabilities sometime later – not only against Ukraine, but also against the West and its critical infrastructure as a punishment for its sanctions and support of Ukraine.

Three months later, this has not happened either. Some experts are still expecting cyberwar to come, just sometime in the future. Others say that they were right, and cyberwar is here, except that the threat in Ukraine was deterred, or that attacks were launched but then neutralized in time.

In contrast, we claim that experts who expect cyberwar to happen keep underestimating the practical limitations of cyberattacks (also called cyber effects operations) and consequently overestimating their strategic value – despite ample empirical evidence that cyberattacks are not very effective at coercive and destructive action.

We aim to correct the distorted cyber threat debate by better grounding it in observable reality. While cyber operations remain important for intelligence operations and mildly disruptive attacks, destructive cyberattacks on key military or civilian infrastructure are challenging to implement and ineffective when compared to conventional attacks. The reason is an operational trilemma that constrains the speed, intensity, and control that cyber operations can achieve – thus limiting their strategic value and rendering catastrophic attacks highly improbable. Policymakers should focus on countering and mitigating actual threats, rather than on catastrophic scenarios that are theoretically possible, yet exceedingly unlikely in practice.

Expectations and Fallacies

Doom scenarios about devastating cyberattacks have plagued policy debates for 30 years and have proven to be

Key Points

- The expectation that cyberwar – a high-level, destructive attack via cyberspace – is imminent is based on a series of misconceptions about what it takes to deliver targeted effects in cyberspace.
- A sober look at the evidence shows that cyber operations are either too slow, too weak, or too volatile to serve as attack tools in military operations. Even in hybrid settings, they offer limited strategic value.
- The policy debate needs to move away from its technological over-fixation and to stop misrepresenting any politically motivated cyber incident as a harbinger of cyber doom.
- Cyber operations are only useful for intelligence gathering or disruptive operations when the timing and severity of the effect does not matter for the success of the operation.

stubbornly persistent. There are two interlinked problems that keep the specter of cyberwar alive:

Table 1: 2014–2017 Cyber Operations

Name	Effects	Strategic Value
2014 Election Interference	Malware disrupted computer systems of Central Elections Commission, but backups prevented impact on vote counting.	Negligible
2015 Power Grid Sabotage	Hackers temporarily disrupted power supply in rural Ukraine by manipulating systems; victims neutralized it within six hours by switching to manual control.	Negligible
2016 Power Grid Sabotage	Malware temporarily disrupted power supply in Kyiv; destructive payload failed, and victims neutralized it within 75 minutes.	Negligible
2017 NotPetya	Self-spreading malware ("worm") irreversibly encrypted data on systems, achieved massive scale, especially affected Ukraine's private sector, spread globally causing collateral damage – including Russian targets.	Significant impact on Ukraine's GDP, collateral damage causes costs to Russia (including sanctions)
2017 BadRabbit	Disk-encrypting malware, works like NotPetya but is reversible, spreads manually and at small scale, causes minor nuisance.	Negligible

The first problem is the inflationary use of the term "cyberwar" for all politically motivated cyber operations. This glosses over important differences concerning the perpetrators, capabilities, and strategic effects. Every incident is read as a proof for rampant vulnerabilities of modern societies and as a harbinger of doom. In this view, cyberwar is already here.

Second, there is no consensus about the likelihood of a high-level, destructive cyberattack on civilian critical infrastructures – the expert definition of cyberwar. By pointing to society's vulnerabilities and from there deducing the high likelihood of doom to come, many still expect it to be imminent. For them, cyberwar will come or is almost here.

Such predictions are guided by four fallacies that stem from ignoring interaction-effects between technology and politics:

The "vulnerability" fallacy: The assumption that when vulnerabilities exist, they will be exploited. In reality, the existence of a vulnerability does not reveal anything about why, how, and when it would make sense for an adversary to exploit it.

The "the hack is the success" fallacy: The belief that the network intrusion, or hack, itself is proof of success. In reality, the success of any operation can only be determined by the political or strategic effects that are achieved through that operation.

The "cheap and easy" fallacy: The belief that cyber tools (software) are a low-risk "weapon" for the weak. In reality, controlled, targeted attacks suitable to reach strategic goals are not cheap and easy but hard, complicated, and risky.

The "just pull the trigger" fallacy: The belief that cyber tools work like conventional arms. In reality, cyber operations usually take months if not years to prepare and deliver. They are not something we can simply "launch" at a whim, and their use requires planning and integration into chains of command.

Technology constrains what is achievable politically, whereas politics constrains what will be attempted technologically. Russian cyberattacks, clearly attributed to the Russian government, in Ukraine since 2014 are an excellent example to demonstrate this both in a hybrid conflict setting and in an actual war.

Evidence from Ukraine, 2014–2022

Russia's aggression against Ukraine since 2014 presents a useful case to examine the effects and strategic value of cyberattacks for at least three reasons. First, Russia is widely held to be one of the world's foremost cyber powers with significant offensive capabilities. Second, from 2014 to 2022 Russia resorted to a strategy of low-intensity aggression enhanced by cyberattacks that many analysts have held to be the future of war. Significantly, such "hybrid war," as it has since been christened, is supposed to be as effective as, if not more effective than, conventional war due to the effectiveness of cyberoperations. Third, Russia has used its cyber capabilities so frequently and in such varied contexts that some observers have described Ukraine as its "test lab for cyberwar." Below we examine the sobering results.

Hybrid War (2014–2017). In this conflict phase, Russia used five disruptive cyber operations against Ukraine (Table 1). These pursued election interference, critical infrastructure sabotage, and economic warfare. While some operations achieved observable effects, a sober look at evidence reveals the shortcomings of such operations. Cyber operations offer unique strategic advantages because they proceed in secret and exploit an adversary's own computer systems to use them against the adversary. As such, they are primarily instruments of subversion rather than war. Yet exploitation involves a distinct set of challenges that create an operational trilemma among speed, effects intensity, and control over effects. Actors can only increase the effectiveness of one of these variables at the cost of losing out across the remaining ones.

This trilemma is clear across Russia's cyber operations against Ukraine, as these operations were either too slow, too weak, or too volatile to produce strategic value.

Table 2: 2022 Cyber Operations

Name	Effects	Strategic Value
Jan 2022 Website Defacements	Multiple UKR government websites temporarily defaced with threatening message, no reported impact on systems.	Negligible
Jan – April 2022 Disk Wipers	Multiple disk wipers (data-deleting malware) infected Ukrainian systems, small to modest scale, no evidence of significant impact.	Negligible
Feb 2022 DDoS Attacks	Distributed Denial of Service Attacks (DDoS) temporarily overloaded websites of UKR government agencies and some banks, causing nuisance but no lasting impact or damage.	Negligible
Feb 2022 Viasat Sabotage	Viasat Satellite Communication Service (used by UKR military) disrupted at the time Russian invasion started. No impact on UKR military communications but collateral damage across Europe.	Negligible
April 2022 Power Grid Sabotage	Attempt to disrupt power supply in Ukraine, detected and deleted before any effect achieved.	None

Even the single exception, the NotPetya malware of 2017 that spread globally and caused massive economic damage, ultimately proved this limitation: Its wide spread was an accident – the hackers lost control over it.

Due to their shortcomings, these operations failed to contribute measurably towards Russia's dual strategic objectives of changing Ukraine's pro-Western foreign policy and undermining public support for this policy. Interestingly, Russia stopped attempting disruptive cyberattacks against Ukraine from 2017. Russia failed to achieve its core objectives through hybrid war. Ukraine maintained its pro-Western foreign policy despite continuing Russian aggression, including its annexation of Crimea and ongoing semi-covert warfare in the Donbas.

War (2022–). Hybrid war had failed, hence Russia changed strategy. In February 2022 it invaded Ukraine, commencing an actual large-scale war. While Russia amassed its troops along Ukraine's border in the preceding months, many analysts predicted that if Russia would invade, it would also unleash cyberattacks of unprecedented destructiveness. As the conflict changed from low-intensity hybrid war to high-intensity conventional war, the theory went, so would cyberconflict.

As before, these expectations built more on theoretical possibilities than strategic realities and practical constraints. The essential point to consider here is that Russia had already tried and failed to achieve its objectives through cyber operations. Strategically, there was thus little reason to expect cyberwar to ramp up once Russia had made the choice in favor of conventional war.

Even if Russia did aim to cause greater destruction through cyber means, doing so requires significant planning, preparation, and resources – foremost, time. None of this was evident. Rather, we witnessed a string of rushed, haphazardly implemented, and outright botched cyberoperations (Table 2).

The operational trilemma predicts that the faster one operates, the lower the intensity of effects, and the greater the risk of control loss. Both constraints are in evidence. Most operations used "fast and easy" yet low-intensity effects like data wiping, website defacements, and DDoS attacks. More complex attacks failed or ran out of control. The attempt to cause a power blackout in April 2022 with the same malware as in 2016 stands out as a complete failure. Meanwhile, a disruption of the Viasat satellite communications network evidently aimed at cutting Ukrainian military communications failed to produce a measurable effect on these communications. Instead, it spread uncontrollably, causing significant collateral damage for the service's other European customers, including thousands of wind turbines in Germany.

Overall, there is no evidence that any of the Russian-sponsored operations or, in fact, any of the operations related to this conflict (including the various hacktivist "armies" that have sprung up) measurably affected the course of the conflict, provided observable tactical advantages – such as sabotaging military equipment or disrupting enemy communications during battle – or produced strategic value.

Reality Check

The constraints posed by the operational trilemma render cyberoperations relatively slow, ineffective, and unreliable. These shortcomings limit their strategic value, both in hybrid and conventional conflict. Yet overestimation of their strategic potential continues, evident most recently in the dramatic warnings of impending cyberwar in Ukraine. These predictions both overestimated what cyber operations can achieve while underestimating Ukrainian defenses.

Due to the cyber-fallacies outlined above, experts continue to misrepresent the utility of cyberattacks, focusing on possibilities rather than considering their actual effects. Hence, in assessing the reports on cyberattacks it remains important to separate hype from reality.

Moreover, most analyses underestimated both the effects of victims' learning – with Ukraine being targeted by Russian "cyber experimentation" for years – and the role of defensive measures. In particular, Ukraine's collaboration with defensive cyber teams from abroad is a potential game-changer that may have prevented hostile cyberoperations from succeeding. This is a point worth examining further.

While we cannot fully rule out severe cyberattacks in the future, we can say with high certainty that due to the nature of the cyberspace domain and the nature of the cyber weapon (techniques of exploitation), these limitations will persist. First, cyber operations will remain unreliable tools, not least because the defender can control the effects an operation can have (through security mechanisms, through redundancies, resilience, etc.). Second, their slow speed, limited intensity, and volatility makes them especially ineffective in urgent and unexpected crises. Third, in contrast, cyber operations will remain useful for stealthy intelligence operations and disruptive operations where the timing, duration, and severity of the effect does not matter for the operation.

Further Reading

Maschmeyer, Lennart / Nadiya Kostyuk, **"There is no cyber 'Shock and Awe': Plausible Threats in the Ukrainian Conflict",** *War on the Rocks,* 08.02.2022.
Brief analysis of plausible cyber threats in case of Russian invasion of Ukraine, challenging cyberwar warnings.

Maschmeyer, Lennart, **"The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations",** *International Security* 46:(2) (2021): 51–90.
In-depth analysis of Russian cyber operations against Ukraine, their strategic role, operational mechanisms, and strategic value.

Dunn Cavelty, M., **"From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse,"** *International Studies Review* 15:1 (2013): 105–22.
Looks at the diverse ways in which cybersecurity is presented as a national security issue in political processes.

Conclusion

Despite continued high expectations, there is mounting evidence of the practical limitations of cyberattacks in both hybrid settings and war. This conclusion particularly applies to cyberwar in the form of targeted destructive attacks. In contrast, we expect low-intensity disruptive operations to continue to plague Western networks, ransomware being a key example (in which there is no need to control timing and effect), and potentially as a direct consequence of the war. The same applies to cyber influence operations used to amplify divisions in societies and to cyberespionage. However, these types of operations do not pertain to the realm of cyberwar. Moreover, the constraints of the trilemma still limit their strategic value.

To determine the geopolitical role and relevance of cyber effects operations, we need to ensure a more fine-grained debate about their limits, their promise, and their actual effects (which include our own reactions to cyberattacks), and consequently the utility of different types of cyberoperations. The hyperbolic term "cyberwar" has distorted the debate for almost 30 years. It is high time to stop waiting for a cyberwar that will not come and to consider the reality of how strategic contexts and political will shape the use of technologies in war and conflict.

Lennart Maschmeyer is a Senior Researcher at the Center for Security Studies (CSS) at ETH Zurich.

Myriam Dunn Cavelty Deputy for Research and Teaching at the Center for Security Studies (CSS) at ETH Zurich.

Policy Perspectives is published by the Center for Security Studies (CSS) at ETH Zürich. The CSS is a center of competence for Swiss and international security policy.

Series Editor: Brian G. Carlson
Issue Editor: Dominika Kunertova
Layout: Miriam Dahinden-Ganzoni

Feedback welcome: PolicyPerspectives@sipo.gess.ethz.ch
More issues and free online subscription:
css.ethz.ch/en/publications/css-policy-perspectives

Most recent editions:
Ceasefire Monitoring and Verification Technology (10/2)
Cyberneutrality: Discouraging Collateral Damage (10/1)
Europe: Greater Autonomy, Better Allies (9/10)
The Role of Value Systems in Conflict Resolution (9/9)
Redesigning Nuclear Arms Control for New Realities (9/8)
NATO's Strategic Concept: Three Do's and Don'ts (9/7)

ISSN: 2296-0244; DOI: 10.3929/ethz-b-000549252