SWP Comment
NO. 23 APRIL 2023

Cyber Operations in Russia's War against Ukraine

Uses, limitations, and lessons learned so far

Matthias Schulze and Mika Kerttunen

One year after Russia's invasion of Ukraine, certain assumptions about the utility of cyber operations during wartime can now be put to the test. Russian cyber salvos opened this war, but they failed to achieve their objectives in the face of a resilient cyber defender. Joint cyber/conventional warfighting is still hard to implement due to its uncertain effects, the potential for spill-over, malware development cycles, and differing operational tempos. Cyber operations against Ukraine have not (yet) achieved major strategic effects in reducing Ukraine's capacity to resist. Additionally, Russian information operations targeting Ukrainian and Western audiences fell on deaf ears. The greatest value of cyber operations therefore still appears to lie in their intelligence and reconnaissance functions.

Since the early 1990s, cyber warfare has been heralded by its proponents as a revolution in military affairs or a perfect weapon of war. Most of these discussions have been theoretical, often focusing on questions of how the application of cyber capabilities might meet or exceed the threshold of an armed attack and thus lead to conventional war. Yet few empirical studies examine the military operational utility of cyber capabilities *during* war. Over the past year of war in Ukraine cyber capabilities have been employed in the midst of a conventional war, allowing us to draw preliminary conclusions about the potential game-changing nature of cyber capabilities when used as an instrument of war.

Three Western schools of thought

Cyber capabilities and wartime strategy

Literature on 'cyber warfare' is usually concerned with the application of cyber capabilities for politico-strategic or even criminal purposes rather than military operational ones. The *strategic cyber war narrative* of the 1990s saw cyber warfare as a next-generation front that would threaten modern society. One of the guiding frames of reference was the "Cyber Pearl Harbor" metaphor: With digital decapitation strikes, the power grid could be shut down, critical infrastructure destroyed, and entire economies brought to a halt all without the need

Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

for physical military force. Within this narrative, cyber operations were seen as a strategic counter-value capability that would target societies with the aim of affecting state behaviour during peacetime. In a nutshell, cyber operations were expected to alter the balance of power in the international system because they were perceived to be superior to conventional force.

As the field matured, however, expectations scaled down. Scholars like Martin C. Libicki pointed out that when it comes to the objectives of war, cyber war cannot disarm, "much less destroy", the enemy. Moreover, in the absence of physical combat and violence, cyber warfare cannot result in territorial gains, which can still be considered one of the primary objectives of most modern wars. Furthermore, it is hard to bend an adversary to one's will — the famous Clausewitzian purpose of war — by relying on digital means alone. Research has also shown that strategic attacks against civilians rarely contribute to war-winning objectives, and secondly, are difficult to orchestrate against thousands of different systems that control critical functions of modern societies. Unlike conventional weaponry, many cyber operations are target-dependent, meaning they cannot be used indiscriminately against any system, which complicates operational planning. Furthermore, with such complex attack chains, there is always the risk of failure and unintended cascade effects that could actually backfire on the attacker.

Cyber capabilities on the battlefield

Since the mid-2000s, cyber warfare has not been seen as a standalone capability that elicits effects independent of kinetic conflict, but rather as a compliment to conventional capabilities. In other words, cyber operations can serve as a *force enabler/multiplier* for conventional capabilities when used in a joint and combined fashion. Here, cyber operations in war are not necessarily measured by their strategic effects but are rather seen as a *counter-force capability* that can be directed against enemy armies. One example is the X-Agent malware that infiltrates targeting equipment that guides artillery fire and then leaks the geolocation of artillery positions to enemy forces, which then directs counter-battery fire. Within this conceptualisation of cyber capabilities, the application of cyber means matches well with the ideals of manoeuvre warfare and paralysing the enemy with surgical or acupunctural strikes.

While studies show that military hardware has plenty of vulnerabilities that can be exploited by cyber operations in theory, in practice, this is hard to operationalise. A study by Nadiya Kostyuk and Yuri M. Zhukov on the use of Distributed Denial-of-Service attacks and kinetic military operations in Syria (2013) and eastern Ukraine (2014) shows that timing is often off in joint operations. Conventional attacks and disruptive cyber operations have different planning times and different operational tempos, which makes it hard to achieve joint effects. Malware, for example, has lifecycles: It must first be developed, tested, and then deployed toward adversary IT to produce effects until it is discovered and mitigated. This takes time, often weeks or months. In principle, a single software update or change in configurations on the part of the defender has the potential to nullify the effect of malware. Malware is much more target-specific than bullets. Lastly, to synchronise its effects with ground operations, malware might need live command and control connections to the outside world, which might be infeasible in a combat environment that employs active electronic warfare interference. Therefore, a cyber operation might be useful in the early stages of war as a type of first strike, but the longer that hostilities last, the harder it is to keep operational stockpiles of functional malware and to maintain backdoor access to adversary systems.

Additionally, it is difficult to coordinate manoeuvres between conventional and cyber forces. First, conflicting goals are an issue: intelligence-oriented actors tend to favour hidden long term access to a system (cyber espionage or presence-based opera-