From the Foxhole: Cyber and Kinetic Conflict in Ukraine

Dr. Aaron Brantly

For years, scholars have debated what cyber war would look like if it arrived. Would it approximate a "Cyber Pearl Harbor," resulting in overheating nuclear power plants, or would it be more mundane?

War has returned with a vengeance to the European continent, and while offensive cyber operations have certainly been part of the overall conflict landscape, their impact has been limited. The reality of cyber conflict has failed to match many of the worst fears of cyber hawks. Instead, it has been an auxiliary function that has played an increasingly important role in two principal aspects of the conflict. First, it has served as a minor operational or tactical shaping mechanism with limited successes to make the kinetic warfighting environment more and, at times, less permissible. Its second and most profound impact has little to do with kinetic effects at all. Cyber-attacks have most impacted the information space as they aim to undermine and expose the opposing sides' narratives within the opposing sides. Because of this, they have served as a rallying cry to communities within and diasporas beyond Ukraine. There is little doubt that there are ongoing cyber-attacks against Ukrainian and Russian infrastructures, yet most attacks have been degradative in nature. The more significant attacks have been exploitive and technically relatively mundane.

It is difficult to answer why this conflict has not seen the forecasted Cyber Pearl Harbor, but it likely stems from several simple and interrelated attributes of conflict in cyberspace. Before delving into these attributes and their impact on Russia's war in Ukraine, it would be helpful to understand what cyber-attacks have transpired in the days leading up to the conflict and the initial conflict period. These activities will be divided into two broad categories. The first category looks at the degradative attacks perpetrated by the Russian Federation and actors supporting the Ukrainian state.

Degradative Attacks:

- On January 13th, 2022, Microsoft identified WhisperGate, a form of malware designed to mimic the appearance of ransomware. However, the malware did not contain a means to unlock encrypted files. Instead, it is thought to be destructive malware meant to undermine the availability of systems. WhisperGate has not been formally attributed as of this writing and has still been seen in the wild on numerous systems, including victims in government, non-profit, and technology-related firms.
- On January 14th, 2022, hackers engaged in Cross-Site Scripting or Injection attacks against the content management system (CMS) Дія (Diia). This attack continued for two days, targeted a vulnerability within the CMS, and replaced site content with political imagery in Russian, Ukrainian, and Polish. The attack was technically unsophisticated but did temporarily disable more than 70 Ukrainian government websites, including the Ministries of Energy, Sports, Agriculture, Veterans' Affairs, and Ecology. The attack was traced to Belarussian APT UNC1151.
- On January 24th, 2022, Belarussian "Cyber Partisans" claimed credit for attacking the Belarussian Railway system with Ransomware. The "Peklo" campaign encrypted servers and databases of the Belarussian rail system BelZhD in an attempt to disrupt Russian military mobilization.
- On February 15th and 16th, 2022, multiple Ukrainian government websites, including the Ministry of Defense and the Foreign Ministry, as well as Ukrainian banks and banking infrastructures, began to suffer from DDoS attacks. These attacks were substantial but of minimal impact, and the services of the banks and the government sites were re-established within two days. The attacks were attributed by the United States, United Kingdom, and Australia to the Russian Federation.
- Also on February 15th, many Ukrainians began to receive SMS Spam in coordination with the DDoS attack listed above. These SPAM messages included disinformation on unspecified technical malfunctions that would limit the ability of Ukrainians to withdraw funds from ATMs. This attack is formally unattributed.

- Just prior to the initiation of kinetic hostilities on February 23rd, 2022, new DDoS attacks targeted Ukrainian banks and ministries. The attacks continued into Thursday the 24th as military hostilities commenced. The Open Source non-profit, Bellingcat, attributed these attacks to the Russian Federation.
- Concurrent with the DDoS attacks against Ukrainian banks and ministries, HermeticWiper, a data-wiping malware, was unleashed against financial organizations and government contractors in Ukraine and spilled over into Latvia and Lithuania. More than 100 organizations were impacted.
- As hostilities commenced on February 24th, 2022, portions of the Internet in Kharkiv and the surrounding Oblast were degraded. The result was an ~25% decline in Internet connectivity, according to NetBlocks.
- On February 28th, 2022, Microsoft identified a new Malware propagating through Ukraine targeting digital infrastructures, including financial, agricultural, emergency services, humanitarian and energy sectors. The malware dubbed the Foxblade Trojan was designed to steal data from a variety of different datasets and is believed to have worked in tandem with information attacks to degrade or undermine information dissemination.

Each of the above attacks sought to degrade the capacity of the state or militaries involved in the Russian war against Ukraine. Eight of the nine attacks were undertaken to the benefit of Russian military mobilization and execution of force, while one attempted to impede that mobilization and impair the future use of force. Each of these attacks constituted minor cyber-attacks with limited tactical and operational utility and no measurable strategic utility. The act of degrading systems has had little to no material impact on the conduct of military hostilities or the organization of military forces in Ukraine by either the Russian Federation or Ukraine. In times of peace, the costs associated with system recovery would be relevant to any discussion of impact. Yet, in the current situation, the relative cost of the impact of cyber weapons when compared to even the most minor costs associated with kinetic weapons skews the relationship. In a whole-of-nation approach, continued efforts to undermine and degrade opposition networks and systems remain of interest. There have been repeated calls to domestic and foreign hackers and hacker collectives to aid the Ukrainian state through perpetrating attacks of any size against the Russian Federation. Prior research on cyber-attacks against Ukraine indicates no strategic and limited tactical and operational utility associated with such attacks. Why such attacks have limited utility across all levels of engagement was addressed in a recent paper, "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations" by Lennart Machesmeyer. In it, he identifies a subversive trilemma that constrains cyber conflict as a result of speed, intensity, and control. As he notes, it is extremely difficult to maximize cyber impacts across all three of these variables.

Due to the constrained time horizons of the conflict in Ukraine, it is unlikely that cyber-attacks in the coming days and weeks perpetrated by non-state actors will be able to maximize across any of the three variables identified by Machesmeyer. Without prior access to 0-days and developed malware, the process of developing and deploying impactful cyber-attacks will be constrained to known exploits and patterns of attack. Such levels of attack are likely to remain primarily within proxy communities with little state oversight. Such communities have already had some reasonable successes (albeit formally unconfirmed). The hacker collective, Anonymous, initiated operations against government agencies in the Russian Federation and claimed they breached the Russian Ministry of Defense (MoD). Many of the emails in the released data dump are no longer active.

If cyber-attacks are not playing a major—or even a minor—role in influencing the conflict through the impairment of military capabilities, what use do they have? Cyber-attacks and cyber activities have a profound and important shaping impact on the information environment. Bits and bytes aren't taking out tanks, but they are slowly wearing down the psychological walls of the Russian Federation. On March 1st, 2022, Anonymous (suspected although not confirmed at the time of writing) hackers compromised multiple Russian TV channels and commandeered their broadcasts to display information the Russian government has tried to keep hidden from its citizens. Cyber-attacks have also targeted most major Russian web-based news outlets and dozens of government sites. These attacks did not remove the sites from the Internet but instead utilized their platforms to broadcast information relevant to the conflict that was not previously being broadcast. As a result, the Russian Federation actively shut these sites down. In response to continued information operations and cyber-attacks facilitating information operations, Russia's communications regulator ordered media outlets to remove reports describing Moscow's violence in Ukraine as an "assault, invasion or declaration of war." The regulator also began implementing restrictions on social media platforms such as Facebook and Twitter.

Beyond cyber-attacks, the war is showing the interconnectedness of global information infrastructures. Voluntary actions by Facebook, Twitter, Google, and numerous other platforms limit Russian propaganda efforts without offensive cyber-attacks. In particular, the demonetization and removal of advertising privileges of content creators from Russia by the major social media platforms are constraining Russian information narratives. Calls on social media to find creative ways around Russian censorship include posting reviews on restaurants and businesses throughout Russia to raise awareness of Russia's actions in Ukraine.

Clausewitz is often quoted as saying, "War is politics by other means." It is important to remember that the political nature of war is influenced by many factors. There remains little doubt that the most substantial impact of war is felt through the employment of kinetic means. Yet, the Ukraine conflict demonstrates that while cyber-attacks might not have a kinetic impact, they have an information impact that raises awareness, shapes narratives, and builds support that results in material resources capable of sustaining or undermining kinetic operations.

DISCLAIMER

The views expressed in the article are those the author and not the United States Military Academy, the Department of the Army, or any other agency of the U.S. Government.

Dr. Aaron F. Brantly is an Associate Professor in the Department of Political Science and Director of the Tech4Humanity Lab at Virginia Tech.