Pre-Soviet Trajectories for Digital Warfare: Situating the Early 2022 Ukraine Cyber Attacks Within Russian-Leninist Information Warfare Analysis

Susanna Cox | CX7
2022.03.22

As Russian troops amassed along the Russian-Ukrainian border in early 2022, and a series of cyberattacks directed against Ukrainian targets–alleged to be attributable to either Russian state actors or hacktivists working with de facto state approval if not outright sponsorship–conversations once again turned to Russia's alleged history of integrating cyberattacks with more conventional means of warfare in so-called "hybrid warfare," a conflict formulation many in the US and Europe, including Ukraine, have found difficult to define precisely: "*Hybrid Warfare is a form of 'unreal warfare', and can be very difficult to define as warfare in the traditional sense. Ukraine's Security Chief concurred, describing Russia's war in Eastern Ukraine as 'a new type of war, a Hybrid War, where armies do not always act as direct aggressors'* (Bachmann and Gunneriusson 2015). Bachmann and Gunneriusson go on to describe some of the means by which parties in Hybrid Warfare may *"act to intimidate"* as other loosely coalesced forces–sometimes including criminal elements–conduct kinetic actions on the ground.

Meanwhile, US media was grappling with its own understanding of cyberwarfare. The Wall Street Journal observed that the apparently deliberately limited damage of the January 2022 attacks had left experts "puzzled" (McMillan and Volz 2022), and the Associated Press noted what it called US President Joe Biden's "blunt" language around potential use of force as a response to cyberattacks, referring to a July 2021 speech in which the President told a group "*If we end up in a war, a real shooting war with a major power, it's going to be as a consequence of a cyber breach of great consequence*" (Bajak 2022).

"Blunt" as it may be, President Biden's language around "real" vs cyber- warfare(s) also hints at critical distinctions between US and Russian understandings of what it means to conduct war–and where cyber fits within overall warfare efforts.

Striking in contrast to US & Western European conceptualizations of cybersecurity and cyberspace, which tend to silo and flatten the cybersphere–both defensively and offensively–into its own separate risk surface, is the multi-modal approach of Russian-style Hybrid Warfare wherein both kinetic and psychological actions are supported by "*a plethora of Russian media-based disinformation and propaganda assets, as well as economic pressure tactics and the use of the information sphere to augment Russia's success*" (Bachmann and Gunneriusson 2015).

Connell and Vogler (2017) further elucidate the relationship between cyber and information warfare (IW) in the Russian conceptualization, specifically cyber's position within the larger IW domain: Information warfare, or *informatsionnaya voyna "as it is employed by Russian military theorists, is a holistic concept that includes computer network operations, electronic warfare, psychological operations, and information operations. In other words, cyber is regarded as a mechanism for enabling the state to dominate the information landscape, which is regarded as a warfare domain in its own right."* In many respects, cyber-as-subcomponent in the service of a particular IW operation is an inherently Russian application of the technology.

This form of fighting has, in theory at least, the potential to severely impact the opponent: in the information sphere-as-battlefield, all actions are potentially magnified as psychological effects against the enemy may originate from any number of sources. For example, the early 2007 DDoS attacks on Estonia, thought to "*constitute the first large-scale coordinated use of cyber capabilities by Russia to affect a strategic outcome in a neighboring state"* had a "significant" impact due to Estonia's early adoption of technology as a source of national pride: "*...at the time, approximately 60 percent of the country's 1.3 million people used the internet regularly and the government considered itself effectively 'paperless.' As Urmas Paet, Estonia's foreign minister at the time put it, "the attacks [were] virtual, psychological, and real"* (Connell and Vogler 2017). Ukraine's understanding of Russian IW tactics as employed in the "real" world differs sharply from that of the United States.

Although many non-Russian analysts use the term "Hybrid Warfare," hinting at prior distinctions among kinetic, psychological ops and cyber, Russia itself does not apparently recognize such a division in its terminology:

Interestingly, Russia itself uses 'generational warfare' and others use terms like 'full-spectrum warfare' to describe the Ukraine conflict. It is clear that the difference in Russian and Western terminology emphasizes the actors' perspectives (Bachmann and Gunneriusson 2015).

This distinction of terms suggests significant differentials in understanding around the role of cyber, the contested nature of the information space in conflict, the Law of Armed Conflict (LOAC), and potentially the nature of modern warfare itself.

While President Putin has arguably used so-called Hybrid or Generational Warfare to great effect globally and specifically in both Ukraine and regional skirmishes leading up to the 2014 annexation of Crimea, the evolution of Russia's doctrinal understanding of full spectrum tactics, including cyber, must be situated within Russia's broader history, beginning in the pre-Soviet era:

It is worth noting that discussions over the employment of non-military measures in Russian warfare are not a novel phenomenon; however, these discussions were not adopted by a critical mass of Russia's military establishment until recent years. Russian military scholars have been expounding on the utility of such measures since before the Communist Revolution…Despite the difference in means, as exemplified by the use of digital technologies today, the strategy

undergirding modern Russian military cyberattacks and information operations was laid over a century earlier (Lilly and Cheravitch 2020).

In an October 2017 anthology, an essay by Stephen Blank placed cyberattacks against Crimea–at that point three years into Russian annexation–in line with the landmark 2008 attacks against Estonia:

Estonian authorities (and others) believe that Russia aimed to incite large enough demonstrations that they would provoke violence. Then, they argue, Moscow could have used the ensuing violence as a pretext for launching an anti-Estonian insurgency that could have justified either direct Russian support for the insurgents or even Russian military intervention, as occurred in Crimea in 2014 (Blank 2017, p. 86).

Also noted is not just the specific flavor of the attacks, but the overall trajectory of these campaigns concurrent with Russian kinetic and political activity in the region:

Though Western audiences might consider such threat assessments and scenarios far-fetched, the Estonians and other neighbors of Russia do not. The resemblances to earlier Soviet operations, the nature of the attacks, and the foreshadowing of the Crimean operation are more than suggestive. Indeed, the use of disaffected ethnic minorities and anger at the Baltic states' "lack of gratitude for independence" are long- standing Russian and Soviet tactics as are the organization of minority or other mass demonstrations (ibid).

In a 2016 report for the Strategic Studies Institute of the US Army War College, Blank referenced Leninist philosophies of Information Warfare, and how Russia's military elite themselves understand this legacy and its impact in shaping contemporary Russian policy:

Writing in 2006-07, Deputy Premier and former Defense Minister Sergei Ivanov indicated Moscow's full awareness of [Information Warfare], and that it…allowed them to update the Leninist inheritance of using Communist parties, fifth columns, and intelligence penetration of targeted societies as weapons in what became the Cold War to obtain political and strategic advantages (Blank 2016, p. 222).

Russian policies, strategies and tactics around the use of cyberwarfare as an integrant of Information Warfare must thus be placed within the context of Russian-Leninist history; as such application of even the most bleeding-edge technologies to Russian-style IW can be understood to continue trajectories established long before the collapse of the Soviet Union.

Viewed through this lens, not only do the January and February 2022 Ukraine cyberattacks fit well within the Russian schema of Information Warfare, but the analysis of the hacks' damage as relatively light may be somewhat premature. The attacks in January featured no real destruction of data, but a defacement intended to elicit fear; and while experts expressed initial relief that the February 14th Distributed Denial of Service (DDoS) attacks were evidently not a smokescreen for more serious breaches, attacks of this nature against large financial institutions (in this case Ukraine's PrivatBank and Oschadbank) are likely to have a significant

psychological impact on the population. While the attacks have not been formally attributed to Russia–and might never be–any response on the part of Europe and/or the US must consider the implications of the Law of Armed Conflict (LOAC) *vis-à-vis* cyberwarfare, and Russian-Leninist understanding of cyber within the Information Warfare context, if they hope to have relevance to the conflict or impact in the region.

References

Bachmann, Sascha, and Håkan Gunneriusson. 2015. “Russia's Hybrid Warfare in the East : The Integral Nature of the Information Sphere.” *Georgetown Journal of International Affairs* 16 (Supp. INTERNATIONAL ENGAGEMENT ON CYBER V): 198-211. https://researchprofiles.canberra.edu.au/en/publications/russias-hybrid-warfare-in-the-east-the-integral-nature-of-the-inf.

Bajak, Frank. 2022. “Tripwire for real war? Cyber's fuzzy rules of engagement.” *AP News*, February 14, 2022. https://apnews.com/article/russia-ukraine-joe-biden-technology-business-hacking-5eadc06062f8c7acfc7b7302ec4c4478.

Blank, Stephen. 2017. “Cyber War and Information War a la Russe.” In *Understanding Cyber Conflict: 14 Analogies*, edited by George Perkovitch and Ariel Levite. N.p.: Carnegie Endowment for International Peace. https://carnegieendowment.org/2017/10/16/cyber-war-and-information-war-la-russe-pub-73399.

Blank, Stephen J. 2016. “Information Warfare a la Russe.” In *Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competition*, 222. N.p.: Strategic Studies Institute, US Army War College. https://www.jstor.org/stable/pdf/resrep11980.11.pdf.

Connell, Michael, and Sarah Vogler. 2017. “Russia's Approach to Cyber Warfare.” CNA.org. https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf.

Lilly, Bilyana, and Joe Cheravitch. 2020. “The Past, Present, and Future of Russia's Cyber Strategy and Forces.” NATO CCDCOE: 2020 12th International Conference on Cyber Conflict. https://ccdcoe.org/uploads/2020/05/CyCon_2020_8_Lilly_Cheravitch.pdf.

McMillan, Robert, and Dustin Volz. 2022. “Ukraine Hacks Signal Broad Risks of Cyberwar Even as Limited Scope Confounds Experts.” *The Wall Street Journal*, January 20, 2022. https://www.wsj.com/articles/ukraine-hacks-signal-broad-risks-of-cyberwar-even-as-limited-scope-confounds-experts-11642683723.

At the intersections of AI, Security, Policy, & People

https://cx7.dev/