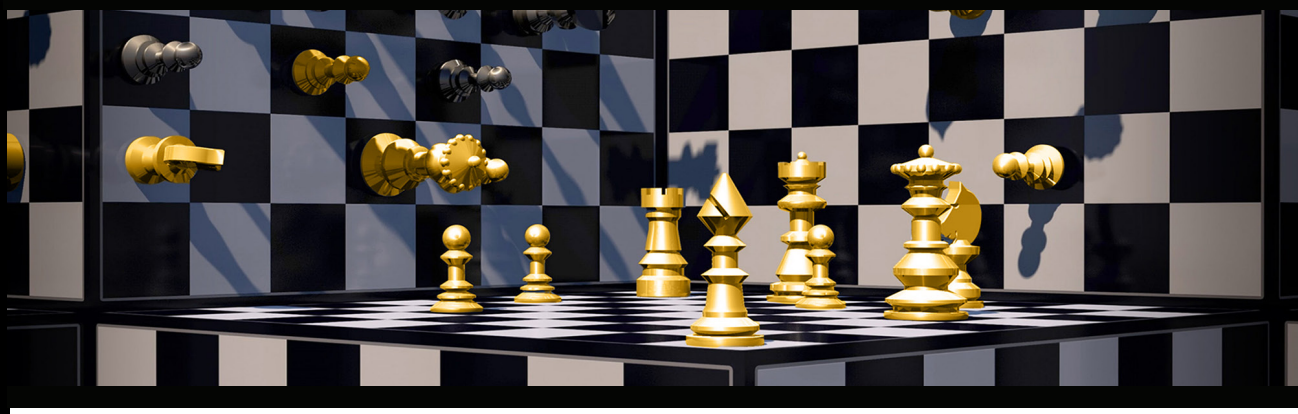

6 November 2023

PERSPECTIVES

The Devil Went Down to Georgia: Executing Cyberspace Resistance to Counter Russia

By Mark Grzegorzewski, PhD, and William Holden

Photo by FLY:D on Unsplash

Amidst the focus on Russia's military engagements in Ukraine over the past year, not enough attention has been given to the cyber resilience needs of other countries on the periphery of the former Soviet Union. Notably, Georgia, Lithuania, and Poland warrant particular attention as they could become the next targets if Russia shifts its focus from Ukraine. Georgia, a victim of a Russian invasion in 2008 and a cyber-driven influence campaign in 2019, presents a compelling case study. Drawing from Ukraine's experiences, Georgia can translate those insights into robust cyber resilience strategies to defend itself against future Russian aggression.

Recommended strategies include forging closer ties with the U.S. to bolster the capacity of Georgia's cybersecurity, re-allocating resources to reduce the impact of Russian cyber operations and activities, and presenting a strengthened front to deter Russian cyber operatives. Moreover, experience is an unparalleled resource, and the Georgians can learn from Ukraine's experience. In fact, there is a strong correlation

between the experience Ukrainian cyber operators gained in the years of cyber conflict following the initial 2014 Russian invasion and today's digital stalemate between Ukraine and Russia. In essence, nearly a decade of conflict honed the Ukrainians resistance capabilities, enabling them to counter Russian cyber operations effectively.

Given its proximity and history, Georgia has likely kept a close eye on how Russia executed irregular warfare in Ukraine since at least 2014, and ideally learned from those experiences to prepare itself for resistance should Russia return. Learning from the Ukrainian experience would enable Georgia to brace itself for Russian cyber effects, especially should a momentarily debilitated Russia seek to reassert its regional dominance by targeting countries within its sphere of influence. Thus, Georgia must be prepared not just for traditional Russian military tactics but also for improved strategies born from lessons learned in Ukraine. In the end, should Russia invade Georgia again, it will not be a replay of what happened in Ukraine. Indeed, it may not even be a physical invasion.

Within the limited scope of this essay, we cannot cover every Ukrainian lesson learned from Russia's invasion relevant to Georgia's resistance. Consequently, we shed light on Russia's cyber operations in Ukraine, which were designed to infiltrate digital infrastructures, shape the information environment, and disrupt and manipulate adversaries. Within this context, we first provide background on the relationship between Russia and Georgia. We then analyze lessons learned from Ukraine in 2022 and assess the effectiveness of Russian cyber capabilities in both Ukraine and Georgia. Based on this evaluation, we highlight the importance of coordinated multi-domain operations and the importance of a well-prepared cyber defense. Finally, we offer suggestions for Georgian cyber resistance, incorporating insights from a 2022 Cyber-Unconventional Warfare (UW) seminar held at National Intelligence University. We conclude by emphasizing the urgency of enhancing Georgia's cyber resilience, given the ever-present threat of a Russian invasion.

Georgia on My Mind

After breaking away from the disintegrating Soviet Union in 1991, Georgia has continuously struggled through a tense relationship with Russia. Eduard Shevardnadze stepped down from his role as the Soviet foreign minister in 1991 due to the Soviet Union's internal chaos, and by 1992, he emerged as Georgia's leader, assuming the presidency in the country's evolving post-Soviet environment. Historically, Russian dominance over Georgia can be traced back to the early 19th century, interrupted only briefly between 1918 and 1921 when Georgia enjoyed a short-lived independence. For Georgians, the future direction of their country is synonymous with safeguarding the state against potential Russian aggression.

To this day, the 2008 Russian invasion over the contested regions of South Ossetia and Abkhazia remains a central point in their bilateral interactions. As background, following territorial disagreements in the early 1990s, Russia mediated a truce, positioning its peacekeeping forces in these contested areas. As Georgia's ambitions for reintegration grew stronger, particularly during Mikheil Saakashvili's tenure (2004-2012) and in a phase when the country was considering joining NATO, Russia perceived this as a direct threat to its security. The 2008 announcement of Georgia and Ukraine's intention to join NATO intensified Russia's concerns, prompting the conflict's escalation. Although the conflict's cause remains debated, Russia swiftly deployed a significant military presence, overpowering the Georgian forces and advancing into Georgian regions within days.

Tensions in cyberspace complemented Russia's physical actions. In fact, Russia's 2008 invasion featured some of the earliest examples of coordinated cyber operations, including Distributed Denial of Service (DDoS) attacks and defacements of Georgian government websites. Even after the official end of hostilities, Russia has used its cyber capabilities to inflict costs on the Georgians any time they have been perceived as moving too closely to the West. Hence, ongoing Russian cyber operations have a historical precedence in Georgia and would likely play a pivotal role in any future Russian aggression towards the country.

Cri-mea River: Russia's strategic miscalculation

The Russian security establishment sees cyber operations as a critical pillar of any operation, as indicated by its 2021 military strategy. This document lays out the concept of strategic operations for the destruction of critically important targets (SODCIT), which uses a combination of long-range fires to inflict damage on an adversary to force them to capitulate to Russian demands early in a conflict. While this damage is generally focused on traditional military means, it also includes cyber operations, particularly where they can impact command of Intelligence, Surveillance, and Reconnaissance (ISR), communications centers, infrastructure, and economics. Thus, Russian military thinking frames cyber operations in the larger context of information conflict, in which sufficient preparation of the information environment leads to sociopolitical conditions in support its objectives.

Before the 2022 invasion of Ukraine, many experts anticipated the conflict between Russia and Ukraine to be short-lived. In principle, Ukraine found itself outmatched, and it was assumed an opening salvo of Russia's cyber operations would overpower and devastate Ukraine swiftly, allowing Russia to showcase its exceptional command in another regional irregular conflict. While this was a possible outcome before the start of the invasion, it is not the situation today in Ukraine. While the Ukrainians suffered some early destructive cyber-attacks against critical infrastructure, such as the attacks on Viasat satellite systems and energy companies, the Ukrainians have also displayed their ability to resist Russian occupation. To the surprise of many, the current Ukraine standstill has revealed how much Ukraine benefited from its many sources of external support.

Outside support to Ukrainian network defense was critical since Kyiv faced an adversary with comparatively immersive cyber capabilities. Possibly to signal Russia, U.S. Cyber Command (USCYBERCOM) publicized that it was supporting Ukraine and had executed Hunt Forward Operations (HFOs) in Ukraine's networks. The fidelity of this support has surely surprised the Russians. Moreover, it has also become clear that U.S. Special Operations Forces (SOF) trained Ukraine personal in the art and science of resistance since at least 2014. The support provided by these two U.S. military organizations, in addition to other U.S. agencies' support, undoubtedly prepared the environment in Ukraine's favor, including in the minds of Ukrainians. This bolstered resilience, both in the tangible and psychological realms, and likely served to counter the potential damage inflicted by Russia's cyber operations and activities, safeguarding Ukraine's critical information infrastructure in the process.

Back in the U.S.S.R.

Russia has a history of using cyber operations to pressure its neighbors, particularly states in its near abroad, which are all former Soviet satellites. These countries are generally targeted by Russia when the Kremlin feels that they are slipping out of Russia's sphere of influence or are perceived to embrace Western democratic values. As such, Russia was not shy about employing cyberspace operations against Ukraine to pull it back into its orbit. Russia has used a variety of cyber operations since the 2014 conflict with Ukraine, including DDoS attacks against anti-Russian organizations, co-opting of social media platforms to minimize anti-Russian rhetoric, and attacking election infrastructure. As the 2014 conflict ground to a stalemate, Russia continued using Ukraine as a sandbox for new cyber and cyber-enabled capabilities and tactics. Notable incidents include cyber-induced power outages in the winters of 2015 and 2016, and the NotPetya attack targeting Microsoft Windows–based systems. As has been widely published, while this malware attack primarily targeted Ukraine, it then spread from intended targets and caused billions of dollars of damage around the world.

Russian forces used cyber operations during the Ukraine invasion across a spectrum of activities, from information operations, espionage, and offensive operations. These efforts were conducted by advanced persistent threats linked to Russia. Some Russian activities were also conducted by and through proxy groups—such as hacktivists, nationalist organizations, and criminal syndicates. From January 2022 to March 2023, the CyberPeace Institute identified 360 Russian cyber incidents against Ukrainian entities, wherein the public administration,

financial, media, and information communication technology (ICT) sectors were targeted by Russian cyber actors. This finding is consistent with the Center for Strategic and International Studies (CSIS) analysis that during its 2022 invasion, Moscow primarily focused on disruptive cyber activities, accounting for 57.4 percent of incidents, while cyber espionage made up 21.3 percent. However, the CSIS report also suggests that despite this Russian activity, "the utility of cyber operations rests in setting conditions and intelligence more than in direct application during large-scale combat operations."

Despite its scope and range, Russia's cyber operations, like the rest of its invasion, failed to produce Russia's desired outcome. Cyber operations did not bring Ukraine to its knees, cripple its economy, or drive it to the bargaining table. Ukrainian cyber defenses proved unexpectedly resilient, and the dramatic effects of anticipated cyberattacks failed to materialize as the Russians were largely unable to coordinate activities in other domains to capitalize on what attacks they did successfully execute. Thus, it is accurate to say, that without ground troops ready to use night vision, causing a citywide power outage merely inconveniences the Ukrainians instead of giving the Russians a strategic advantage in the darkness.

Considering the Ukrainian invasion, the efficacy of Russian cyber warfare seems to have been questionable. What caused this discrepancy remains uncertain. Could it be the swift integration of external support? Or the invaluable experience accrued by Ukrainian cyber defenders over the years? Alternatively, the shortfall might be attributable to Russia itself—due to ineffectiveness in pairing cyber exploits with activities in another domain. It might even be attributed to a Russian intent to preserve Ukrainian infrastructure for their own use. As Russia refrained from dismantling a significant portion of Ukraine's ICT infrastructure during the invasion, countries like Georgia should consider cyber resilience strategies to prepare for how Russia might approach their own ICT assets in a future confrontation.

Midnight Train(ing) to Georgia

Recognizing that Georgia currently is not in a current conflict with Russia, it might seem unnecessary to plan for another Russian incursion. Nevertheless, it is imperative for Western countries to collaborate with Georgia during the "Phase Zero" stage, focusing on cyber resilience to foster a strong deterrence mechanism that could potentially prevent a future Russian provocation.

The concepts of Phase Zero and resistance are distinct but also similar in that they both emphasize pre-conflict shaping of the environment, relationship building, non-kinetic activities, and leveraging local insights. Phase Zero comes before the four-phase military campaign model: deter/engage, seize initiative, decisive operations, and transition. Phase Zero operations are "everything that can be done to prevent conflicts from developing in the first place… consist[ing] of shaping operations that are continuous and adaptive… to promote stability and peace by building capacity in partner nations that enables them to be cooperative, trained, and prepared to help prevent or limit conflicts." Activities within the Phase Zero stage have direct impacts on the way any future conflict would play out.

Resistance is "an organized effort by some portion of the civil population of a country to resist the legally established government or an occupying power and to disrupt civil order and stability." It is a part of the theory of Unconventional Warfare, defined as "activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla force in a denied area." To be effective in integrated deterrence through unconventional warfare, USCYBERCOM must be proactive and continuously engaged during Phase Zero. Additionally, both SOF and USCYBERCOM need to maintain constant readiness to allies and partners ahead of conflict, ensuring that they can provide support over the long term whenever required. This commitment equips allies and friends to deter against potential invasion. Waiting until Russian tanks roll across the border is much too late. Therefore,

SOF should maintain regular contact with potential resistance entities, and concurrently, USCYBERCOM should proactively probe networks and persist within digital networks.

Pre-invasion activities associated with both Phase Zero and the first step in the UW model emphasize relationship-building with local entities, from government officials to grassroots movements. While these activities can involve combat, the focus is on non-combat initiatives such as training, advising, liaising, and information sharing. Likewise, deep local insights, cultural sensitivities, and socio-political dynamics are crucial to inform both strategies.

In the interconnected world, integrating these time-tested strategies with cyber enabled-operations (with local characteristics) is paramount. However, the U.S. defense community must first understand the other's language. One significant observation from the 2022 Cyber-Unconventional Warfare seminar hosted at National Intelligence University was that the two communities, SOF and cyber, often spoke different languages when referring to similar concepts, such as Phase Zero and the preparation phase in the Unconventional Warfare model. After establishing a common vernacular, ensuing discussions presented suggestions that could be integrated into both Phase Zero and the preparation phase of UW phases to enable cyber support for resistance.

For instance, to lay the foundation for effective resistance, it is essential to first grasp public sentiment, build robust communication infrastructures, recruit allies, and adequately equip resistance forces. In addition, by analyzing public sentiment, narratives can be crafted to align with local concerns. Virtual personas might serve as invaluable channel for distributing information, gathering intelligence, and infiltrating opposition networks. Through consistent and meaningful messaging, the public's perspective can be shaped, making them more receptive to external support. Finally, prioritizing secure communication platforms can strengthen resistance recruitment, and ensure the consistent provision of required resources.

When considering cyber-integrated resistance, initiating relationships with resistance groups or governments-in-exile requires creativity since meeting in-person may not be feasible. Using methods like flash mobs can be a way to assess public mood, spot potential allies, and carve out discreet communication pathways. Collaborating with key local influencers can help shape public sentiment to resonate with overarching objectives. Capitalizing on digital platforms catering to online gamers to engage younger audiences or even growing discrete messaging channels could empower digital outreach initiatives in alignment with both the resistance and U.S. objectives. These platforms could also be used to strategically spotlight the flaws of an invading force, creating an atmosphere ripe for resistance.

Considering Russia's historically persistent regional aggression, the U.S., Georgia, and NATO must remain vigilant. Events in Ukraine are not isolated. They are indicative of Putin's broader territorial aspirations. For that reason, enhancing Georgia's cyber resilience capabilities against potential Russian maneuvers is of utmost importance to guard against and prepare for future Russian aggression.

Wind of Change

Given Russia's intrusion into Ukraine, it is vital for the U.S. to collaborate with countries vulnerable to Russian aggression, such as Georgia, to enhance their cyber resilience, focusing on safeguarding their cyber infrastructure in key areas like command structures, ISR, communications, and other important infrastructure. Partnerships with Western countries, private sector entities, and other non-governmental organizations are also vital to preserve Georgia's digital capabilities. Collaborative efforts should concentrate on developing robust defenses against cyber threats while also formulating resilience strategies.

Ukraine's ordeal underscores that isolated cyber victories, such as significant power outages, may not equate to strategic achievements, unless they are aligned within a broader military strategy. Considering this, Georgia

should broaden its approach beyond a purely technical focus on cyber and focus on the interdependencies between public administration, finance, media, economics, and the ICT. All must be fortified against cyber threats, while the public workforce must be informed about potential cyber risks. By enhancing these segments and elevating public recognition of cyber risks, Georgia can mitigate the societal and economic impacts of potential Russian cyber operations and activities.

Both Phase Zero and Resistance emphasize pre-conflict preparation, relationship cultivation, and non-combative measures that capitalize on local knowledge to further U.S. goals. Phase Zero seeks to preempt conflicts by fostering stability, whereas Resistance attempts to resist the overthrow of a legitimate government. To support friends and allies, entities like SOF and USCYBERCOM should consistently be ready, prioritizing proactive and sustained involvement rather than reacting to explicit acts of aggression. The blending of cyber operations is pivotal in fostering resistance in the digital realm, gauging public sentiment, and modifying communication for optimal resonance. Employing innovative tactics in cyber-enabled resistance can establish alliances, influence public sentiment, and bolster other resistance efforts, all while remaining alert to challenges from hostile countries. Essential to Georgia's national defense, the U.S. must advocate for Georgia to augment its cyber resilience, incorporate lessons learned from Ukraine, and integrate Phase Zero cyber activities and resistance approaches. This approach will ensure that Georgia not only endures in the modern digitally connected world but also flourishes, staying ahead of Russian hostility.

About the Authors:

Dr. Mark Grzegorzewski is an assistant professor of cybersecurity at Embry- Riddle Aeronautical University in the Security Studies and International Affairs Department. He is also an Army Cyber Institute Fellow.

Capt. William "Stone" Holden is a Marine Officer currently assigned to United States Southern Command (USSOUTHCOM), where he has held billets in security cooperation and collections management, as well as managing a variety of projects that implemented cutting-edge technological solutions to address a range of threats in USSOUTHCOM. He previously served in Indo-Pacific Command (USINDOPACOM) with 3rd Mar Regiment and Combat Logistics Battalion 3.

The views expressed in this article are those of the authors and do not reflect the official policy, opinion, or position of the Department of Defense, Defense Security Cooperation Agency, the Irregular Warfare Center, U.S. Special Operations Command, or the authors' employers.