An Intelligence Officer's Perspective

CPT STEPHANIE J. SEWARD

The United States recently entered a new era of aggressive competition with an old rival, Russia. Russia previously pioneered the development of ever bigger and better atomic and hydrogen bombs in a race to gain dominance. Both the U.S. and Russia participated in proxy wars worldwide to gain leverage and influence. The emerging competition analogously still involves proxy conflict and incorporates second strike capability. However, the current clash is much colder than the first, lacking many of the kinetic aspects of physical engagements. While the threat of nuclear warfare still persists, the current conflict focuses on the technology that now permeates every aspect of our lives. The U.S. is involved in a new era of cyberwarfare conducted at a national level. During the Cold War, the U.S. used its economic and military prowess to overpower the Soviet Union. Throughout the current clash, military might is as important as ever. As such, the U.S. Army must arm itself to overcome cyber threats from the strategic to the tactical level. In this competition, the Army must synergistically integrate cyber awareness, capability, and capacity to the pinnacle of tactical operations.

Russia's recent actions in Georgia and Ukraine illuminate Russia's cyber capabilities and expose its motives. Both Georgia and Ukraine are satellite nations with strong ties to Russia socially, ethnically, and diplomatically. Before Russia's kinetic engagements, each nation moved toward the protection of the West to align with NATO ideals, policies, and economic benefits. As a result, Russia and associated non-state actors, conducted cyber activities to influence these two nations. Ultimately, Russia conducted kinetic operations against both nations. However, the initial stages of Russia's invasions used a relatively new form of attack: cyberwarfare integrated with information warfare (INFOWAR).

Background: Cyber Component of INFOWAR

U.S. Army doctrine defines INFOWAR as "specifically planned and integrated actions taken to achieve an information advantage at critical points and times. The goal of INFOWAR is to influence an enemy's decision making through his collected and available information, information systems, and information-based processes, while retaining the... ability to employ the same."[1] Russia's conception of INFOWAR is broad

reaching. Russia seeks to "control information in whatever form it takes..." through subversive means.[2]

Russia does not merely engage in INFOWAR in the cyber theater. Rather, Russia seeks to control public opinion and attitudes towards its actions during peaceful operations, both within and outside of the cyber realm. In fact, Russia's INFOWAR philosophy indivisibly harmonizes Russia's cyber and INFOWAR efforts with kinetic operations. MG Stephen Fogarty, former head of the Cyber Center of Excellence at Fort Gordon, GA, emphasizes, "It's not just cyber, it's not just electronic warfare, it's not just intelligence, but it's really effective integration of all these capabilities with kinetic measures to actually create the effect that their commanders [want] to achieve."[3] In a time of conflict, Russia will escalate its INFOWAR operations in all mediums to destabilize the affected populace and target key politicians, critical infrastructure, and even individual soldiers.[4]

Likewise, Russia uses non-attributable hacking as a primary INFOWAR weapon. For instance, Georgian technicians could not conclusively prove that Russia was behind the hacks initiated before its invasion of Georgia in 2008. In response, Georgian National Security Council Chief Eka Tkeshlashvili stated, "There's plenty of evidence that the attacks were directly organized by the government in Russia," when referencing how the attacks coordinated with military action.[5] Regardless of the strong evidence for Russia's involvement in the cyberattacks, even Tkeshlashvili recognized the predicament non-attributional hacking had created. "I'm not saying it's enough for a criminal court, to prove a case beyond a reasonable doubt," she said.[6] When engaging in network attacks, hackers can easily hide their identities in numerous ways. A skilled hacker can perform an attack through specific means that render attribution attempts futile; the hacker can also frame other hackers or nations.[7] However, attribution, or lack thereof, does not directly affect actions at the tactical level. Russia demonstrated in Georgia that, regardless of the source, hackers coordinated attacks with Russian military action.[8] Correlative activity matters to the military at the tactical level while attribution matters to strategic and national players. Thus, analysis here focuses on how Russia's conceptual and doctrinal cyber integration evolved through escalating attacks on Georgia and Ukraine.

Cyberattacks as Indicators of Kinetic Action in an Integrated Attack

Initial cyber operations in Georgia focused on discrediting the government and validating Russia's actions. Before Russia implemented any blockades or dropped any bombs, cyber actors targeted news and government websites that spread information for the area that Russia would later inundate with kinetic action. Hackers specifically exploited websites designed to protect civilians and spread information.[9]

Reflecting the tactics and strategy used in the conflict, Training Circular (TC) 7-100, *Hybrid Threat*, provides commanders and intelligence leaders with a framework for understanding the Russian adversary. TC 7-100 illustrates tactics a hybrid threat (HT), like the Russians, use when influencing the battlespace. The Army's shared understanding of threat operations detailed in the TC illustrates the predictability these early cyberattacks provided for kinetic operations. In Georgia specifically, Russia's tactics reflected the HT's disruption zone operations as outlined in TC 7-100.

Russian hackers implemented cyber efforts in Georgia primarily during the disruption zone effort. Disruption forces can "[d]isrupt enemy preparations or actions. Destroy or deceive enemy reconnaissance. Begin reducing the effectiveness of key components of the enemy's combat system."[10] In Georgia, cyber disruption elements, integrated with INFOWAR operations, demonstrated these capabilities.

Russia initially targeted large-scale media outlets and government websites nationwide at least three weeks before the kinetic attack, disrupting Georgian preparation for the invasion. These initial hacks served as rehearsals for focused cyberattacks later in the conflict.[11] In the days and hours leading up to kinetic strikes, Russia's hackers targeted media and communications in the areas they subsequently invaded. More serious, longer-lasting attacks began just before kinetic engagement. "Official sites in Gori, along with local news sites, were shut down by denial-of-service attacks before the Russian planes got there."[12]

Before hackers exploited national websites, they dismantled Georgian hacking groups, effectively destroying Georgian cyber reconnaissance capabilities. Afterwards, Georgia could not anticipate or defend against Russia's cyberattacks. This occurred at a strategic/operational level; Georgia did not have cyber assets at tactical levels.[13]

However, in a fight against a near-peer nation, hackers may initially neutralize national-level cyber efforts in conjunction with national media targets. Subsequently, hackers could shift focus to local tactical assets and local media assets.

Hackers targeting Georgia did not destroy key components of Georgian combat systems. Georgia simply did not have enough advanced technology to allow Russia to exploit vulnerabilities in key systems. While Russia did target communications in Georgia, it did not reduce key components of Georgia's combat systems. Cyber actions in Georgia were relatively simplistic compared to those undertaken in Ukraine.[14]

As such, Georgia provides an excellent framework to illustrate lessons learned for the U.S. Army before graduating to the more complex battlespace in Ukraine. Tactical commanders operating in theater should understand that they are within weeks of kinetic engagement when widespread attacks targeting civilian media communication nodes and government websites begin occurring against a nation. As in Georgia, hackers will look to shut down key communication lines that facilitate civilian movement to safety. Additionally, once a commander's specific area of operations loses civilian communication capabilities and hackers neutralize local news and government sites, kinetic action is imminent in that area. In other words, if commanders begin receiving reports that their cyber warriors are defending against a sudden

increase in the number of attacks designed to neutralize their counter-strike and detection capabilities, their troops are likely targets for kinetic action. Georgia underwent such attacks at a national level and lost its capability to respond to or anticipate cyberattacks.

Cyberattacks and Irregular Warfare: The Ukraine Conflict

Experts agree that Russia is using Georgia and Ukraine as testing grounds for cyber strategies and to demonstrate cyber capabilities.[15] However, the scale of cyberattacks in Ukraine far exceeds the cyberattacks against Georgia. Between October and December 2016, Ukraine endured more than 6,500 cyberattacks on 36 targets. Every part of Ukraine has felt the effects of the attacks.[16] Additionally, after repeatedly targeting other Western nations, Russia recently admitted to a large-scale cyber and INFOWAR effort. Russian Defense Minister Sergei Shoigu recently stated, "We have information troops who are much more effective and stronger than the former 'counter-propaganda' section" while highlighting the intelligence and effectiveness of new INFOWAR initiatives.[17]

The cyber and INFOWAR attacks in Ukraine correspond with the unconventional warfare model of the HT. Unconventional warfare "encompasses a broad spectrum of military and paramilitary operations which are normally of long duration and usually conducted through, with, or by indigenous or surrogate forces."[18] As such, irregular forces incite kinetic violence and use asymmetric warfare techniques.[19]

In this case, Russia engaged in or encouraged irregular, non-uniformed separatists to take violent and non-violent action in Ukraine. Identifying general trends or alignment of strategy with an overall threat structure in the irregular warfare theater is somewhat more challenging than in the conventional context. As a result, the enclosed analysis of the cyber portion of the Ukrainian crisis will focus on anecdotal examples of cyber capabilities before drawing broad-scale conclusions.

Background on Fancy Bear and the GRU

A hacking organization referenced as Fancy Bear was likely behind most, if not all, of the attacks discussed in the next section. Fancy Bear is not necessarily an arm of Russia's government or military; however, its actions correspond with the Главное Разведывательное Управление (Glavnoy Razvedevatelno Upravlene [GRU]), Russia's primary foreign intelligence agency.[20]

Tactical Danger of Cell Phones: Anecdotal Examples

The first anecdote revolves around a legitimate application named Попр-Д30.apk (Popr-D30) developed for Android devices. The application uses basic algorithms to mimic our Advanced Field Artillery Targeting Direction System (AFATDS) and reduces the targeting time for the Ukrainian D-30 122mm artillery piece from minutes to under 15 seconds. Around 9,000 artillery personnel used the application.[21]

Unconventional warfare "encompasses a broad spectrum of military and paramilitary operations which are normally of long duration and usually conducted through, with, or by indigenous or surrogate forces."[18] As such, irregular forces incite kinetic violence and use asymmetric warfare techniques.[19]

Fancy Bear developed a hack called X-Agent to exploit the Android application. X-Agent allowed intelligence analysts to read messages sent via the application and the phone used to potentially identify chain of command within the unit, unit composition and disposition, as well as future operations. Additionally, X-Agent appears to allow Fancy Bear to roughly identify the location of the D-30 artillery pieces. As a result, Russian strikes destroyed approximately 80 percent of Ukraine's D-30 arsenal.[22]

Using hacks like X-Agent, hacking groups can gather cell phone numbers from exploited phones. In some instances, INFOWAR agents supposedly gathered phone numbers and sent text messages directly to Ukrainian soldiers' phones encouraging them to defect.[23] INFOWAR groups can collect cell phone numbers through nefarious and normal means. However, hacks may give threats, like the GRU, access to unit call rosters stored on phones. The GRU and other agencies then send targeted soldiers messages to defect, propaganda, or even impersonate another soldier or family member to distract the soldier from warfighting.

The devastation caused by the Popr-D30 cell phone hack confirms that tactical leaders should not allow cell phones on the new battlespace. If forced to allow cell phones, commanders must strictly control (as best they can) which applications soldiers download and employ. X-Agent was also used in the hack that targeted the Democratic National Committee before the 2016 election. It is extremely flexible, and Fancy Bear can use it on numerous applications.[24]

Social Media Attacks

Recent reporting reveals that Russia's INFOWAR agency has manipulated individual soldiers' social media profiles. Attackers pose as a trusted source to a soldier (presumably as a fellow soldier or family member). There is limited information available about what the "trusted source" communicates to the affected soldier. However, the potential is extremely damaging and broad sweeping. Unconfirmed reports demonstrate that INFOWAR agents encourage soldiers to defect or allege nonexistent family issues to distract the soldier from warfighting.[25]

Many leaders will note that short message service (SMS) and social media attacks are not necessarily the result of hacking and therefore are not related to cyberwarfare. Russia views such attacks differently. Russia's INFOWAR and cyberwarfare efforts are so closely integrated that, from Russia's perspective,

it is hard to distinguish between the two.[26] Thus, such INFOWAR attacks are part of a single overall objective; hackers can initiate them via cyber means.

Additional Tactical Considerations

• **Commanders should practice full analog days during tactical training exercises.** For Russia, cyberwarfare is intimately associated with targeting and electromagnetic warfare considerations. Though not discussed above, tactical leaders should still consider the effects of GPS and communications jamming throughout tactical operations. Additionally, the enemy's ability to target computer systems may deny commanders use of mission command systems. U.S. Army forces need to train accomplishing all mission-essential tasks in a low to no communications-enabled environment.

During field training exercises, commanders should require their command posts (CPs) to maintain redundant analog systems for all operations. Then, without warning, commanders can require their CPs to rely only on specific communications platforms while eliminating the CP's ability to digitally track. For instance, the commander would say that FM radios are jammed and all communications must occur through other means. Concurrently, the commander might disable all computer systems within the CP. Such an exercise would force leaders and Soldiers to use high frequency communications and vehicle-mounted Blue Force Trackers (BFTs) exclusively. This training would also limit the effectiveness of cyberattacks on command nodes, reducing the enemy's willingness to invest resources in executing such attacks.

• **Commanders should advocate for real-world cyber training and take full advantage of that training when offered.** Intelligence, cyber, and maneuver Soldiers need to train against an enemy who exploits SMS, social media, and cell phone applications. This exercise allows commanders and staffs to train and to suggest offensive and defensive action U.S. forces could take against a new generation enemy.[27] This provides Soldiers experience with potential INFOWAR attacks so that they can discriminate attacks from legitimate information in real time. Additionally, such action familiarizes intelligence Soldiers with patterns to look for in enemy INFOWAR attacks and exposes cyber warriors to potential exploits.

• **Cyberattacks are generally a support element for another effort.** Cyber enables other operations. Generally speaking, cyberattacks do not harm Soldiers directly or destroy infrastructure. Instead, offensive cyber enables other attacks.[28] After a cyberattack occurs, commanders must immediately ask themselves what the enemy's next step is. The cyberattack is merely an indicator of follow-on operations. For example, Russia's cyberattacks in Georgia preceded conventional attacks in the same geographic location.

• **Physical and electronic security is of utmost importance.** Commanders must remember that if an enemy has accessed one part of their network, the enemy has access to all of their network. As the severity of the kinetic attacks on Ukraine increased, Russia also increased the scale of its attack on infrastructure. At one point, hackers shut down a portion of Ukraine's power grid equivalent to the size of the state of Massachusetts, and the hackers could have shut down more.[29] That is the power of networks; once the hackers had access to one component, they could affect the whole system. If an unauthorized person can enter the commander's CP and insert an unauthorized disk, or if a Soldier fails to update his computer when required, the enemy can gain access to the entire network.

Photo by Steve Stover

Cyber operations specialists from the Expeditionary Cyber Support Detachment, 782nd Military Intelligence Battalion (Cyber), Fort Gordon, GA, provide offensive cyber operations during a training rotation at the National Training Center at Fort Irwin, CA, on 18 January 2018.

• **Remember that anything that uses signals or connects to a network is vulnerable.** Recent reports demonstrate that Russian electronic warfare assets can predetonate or dud incoming artillery and mortar rounds' electronic fusing.[30] As commanders identify potential electronic assets to deploy in tactical operations, they need to consider each asset's vulnerability in their risk management.

• **The enemy can monitor a commander's communications at all times.** "Russian electronic warfare can detect all electromagnetic emissions, including those from radios, Blue Force Tracker, Wi-Fi, and cell phones, which can then be pinpointed with unmanned aerial systems and targeted with massed artillery."[31] As demonstrated by the Popr-D30 application, hackers can exploit cell phones and communications. Additionally, Russia can monitor unencrypted communications from mission command systems. Commanders must encrypt their communications while ensuring that Soldiers guard those encryptions and practice net jump procedures to avoid exploitation. Commanders should also note that the enemy may monitor their communications and locations without exploiting them for intelligence value. As such, commanders should change encryptions as required by the operating environment and limit long periods of communications, especially over FM.

• **Commanders must integrate cyber enablers at all levels.** Incoming cyber warriors are working on understanding and communicating with maneuver counterparts. Maneuver commanders need to ensure they understand what cyber enablers bring to the fight. Commanders who understand cyber enablers can drive requirements at all levels. Commanders must also accept that as cyber integrates with the force, they will encounter civilians and Soldiers alike from numerous different agencies and backgrounds. It is incumbent upon commanders to build relationships and integrate these individuals as the Army develops multi-domain capabilities.[32]

"We haven't had the cyber Pearl Harbor the way that we thought, in some way because cyberattacks tend to only take down things made of... silicone... and those things are easy to replace... So I'm not one of those [who] think cyberattacks have been that bad lately... because no one has died yet... I think that we will look back on these days as the halcyon days, when Americans have not yet started dying [from these attacks]."[33] Just as U.S. military prowess overcame Cold War threats, increasing our understanding of the current threat operating environment prepares the tactical Army for potential future conflicts.

Notes

[1] Training Circular (TC) 7-100, *Hybrid Threat*, 2010.

[2] Keir Giles, "The Next Phase of Russian Information Warfare," NATO Strategic Communications Centre of Excellence, 2015, 2.

[3] Sydney J. Feedberg Jr., "Army Fights Culture Gap Between Cyber & Ops: 'Dolphin Speak,'" *Breaking Defense* (10 November 2015). Accessed 8 August 2017 from http://breakingdefense.com/2015/11/army-fights-culture-gap-between-cyber-opsdolphin-speak/.

[4] Ibid.

[5] Noah Shachtman, "Top Georgian Official: Moscow Cyber Attacked Us -- We Just Can't Prove It," *Wired* (11 March 2009). Accessed 17 July 2017 from https://www.wired.com/2009/03/georgia-blames/.

[6] Ibid.

[7] Ibid.

[8] Bob Killebrew, "Russia-Georgia: Early Take," *Small Wars Journal* (15 August 2008). Accessed 10 August 2017 from http://smallwarsjournal.com/blog/russia-georgia-early-take.

[9] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*. Accessed from http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.

[10] TC 7-100.

[11] Hollis, "Cyberwar Case Study."

[12] Shachtman, "Top Georgian Official."

[13] Hollis, "Cyberwar Case Study."

[14] Michael Connell and Sarah Volger, "Russia's Approach to Cyber Warfare," Center for Strategic Studies, CNA Analysis & Solutions, 2017. Accessed from https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf.

[15] Ibid.

[16] Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar," *Wired* (20 June 2017). Accessed 31 June 2017 from https://www.wired.com/story/russian-hackers-attack-ukraine/.

[17] "Russian Military Admits Significant Cyber-War Effort," *BBC News*, 23 February 2017. Accessed 21July 2017 from http://www.bbc.com/news/world-europe-39062663.

[18] TC 7-100.

[19] Ibid.

[20] Crowdstrike Editorial Team, "Who is Fancy Bear?" *Crowdstrike* (12 September 2016). Accessed 8 August 2017 from https://www.crowdstrike.com/blog/who-is-fancy-bear/.

[21] Adam Meyers, "Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units," *Crowdstrike* (22 December 2016). Accessed 8 August 2017 from https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/.

[22] Crowdstrike Global Intelligence Team, "Use of Fancy Bear Android Malware in Tracking of Ukrainian Field Artillery Units," *Crowdstrike*. Accessed from https://www.crowdstrike.com/resources/reports/idc-vendor-profile-crowdstrike-2/.

[23] Giles, "The Next Phase of Russian Information Warfare."

[24] Ibid.

[25] Ibid.

[26] Connell and Volger, "Russia's Approach to Cyber Warfare."

[27] Dr. Peter Singer, "Cyber Warfare in the 21st Century: Threats, Challenges and Opportunities," Committee on Armed Services, video, 44:30. Accesssed from: https://armedservices.house.gov/legislation/hearings/cyber-warfare-21st-century-threats-challenges-and-opportunities.

[28] Martin Libicki, "Cyberdetterence and Cyberwar," Project Air Force, Santa Monica: RAND, 2009.

[29] Greenberg, "How an Entire Nation."

[30] Phillip Karber and Joshua Thibeault, "Russia's New-Generation Warfare," Association of the United States Army, 20 May 2016. Accessed 10 July 2017 from https://www.ausa.org/articles/russia%E2%80%99s-new-generation-warfare.

[31] Ibid.

[32] Feedberg, "Army Fights Culture Gap."

[33] Jason "Jay" Healey, "Cyber Warfare in the 21st Century: Threats, Challenges and Opportunities," Committee on Armed Services, video, 43:03.

At the time this article was written, **CPT Stephanie J. Seward** was attending the Maneuver Captains Career Course at Fort Benning, GA. She is currently assigned as the incoming 2nd Battalion, 12th Infantry Regiment S2 in the 2nd Infantry Brigade Combat Team, 4th Infantry Division at Fort Carson, CO. Her previous assignments include serving as a multi-functional team platoon leader with the 502nd Military Intelligence Battalion, 201st Battlefield Surveillance Brigade, Joint Base Lewis-McChord (JBLM), WA; and assistant S2, 4th Battalion, 23rd Infantry Regiment, 2-2 Stryker Brigade Combat Team, JBLM. She graduated from the U.S. Military Academy at West Point, NY, with a bachelor's degree in philosophy, minor in applied statistics (nuclear engineering track).