But Like…What Did It DO?: Assessing Russian Cyber Effects in Context

Captain Patrick 'HOWLER' Meissner

"Opinions, conclusions, and recommendations expressed or implied within are solely those of the author and do not necessarily represent the views of the Air University, the United States Air Force, the Department of Defense, or any other US government agency."

In the context of the National Security Strategy's conception of "great power competition" (Trump 2017), perhaps no nation-state has been as aggressive within the cyberspace domain as the Russian Federation. Furthermore, following two Russian campaigns to seize portions of Ukraine and Georgia's sovereign territory, the question may not be if, but when will Vladimir Putin choose to annex another neighbor's land. The Baltic states, for example, have received much of the same pre-crisis attention from Russia that Ukraine and Georgia did, and their annexation would further Putin's apparent strategic goal to re-establish buffer states between Russia and NATO (Galeotti 2019). An escalatory crisis scenario in the Baltics will most likely follow the pattern exhibited in both Georgia and Ukraine. Building on pre-existing divisions within a region, such as between Russian-speaking minorities and the central government, Russia will utilize both real and imagined incidents to further increase tension. As the tensions escalate and inevitably erupt in violence, Russia will seize the opportunity to maneuver ground forces onto key terrain. These maneuvers will be simultaneously denied, misattributed to local 'patriots' and claimed as mere 'peacekeeping' forces meant to protect Russian speaking minority groups. Then, with their strategic end state all but achieved, Russian leadership will call for peace and diplomacy. This sequence of operations appears to be Vladimir Putin's playbook to rebuild the Soviet era buffer states and 'Sphere of Influence' in eastern Europe (Cunningham 2020). Given that Russian cyber capabilities have demonstrably created strategic advantage via the information domain, tactical advantage by exploiting network-centric nature of adversaries, and operational advantage by creating asymmetric opportunities for conventional force maneuvers, US commanders and planners must be

prepared to contest the information domain, fight in a degraded information environment, and train both with and against realistic, meaningful cyber effects to prevail in future conflicts.

In both Georgia and Ukraine, the United States and NATO did not intervene in any meaningful way to thwart Russia, in part due to the unprecedented level of information warfare. As Russian forces moved to secure South Ossetia, Georgian government websites, media outlets, and public facing infrastructure were targeted repeatedly with Distributed Denial of Service (DDoS) attacks, rendering them inaccessible for periods ranging from minutes to hours (Deibert, Rohozinski and Crete-Nishihata 2012). In conjunction with a robust strategic messaging campaign, these cyber-attacks enabled Russia to control the information narrative of the flow. Expanding on this success, the mobile devices of Ukrainian parliamentary members were specifically targeted with both an Internet Protocol (IP) and telephony-based denial while Russian forces moved to seize telecommunications infrastructure within Crimea (Geers 2015). While technologically simplistic, Russia's cyber-attacks sowed uncertainty and created decision disadvantage for Georgian and Ukrainian leadership at a pivotal moment. In any future conflict, it is almost certain that Russia will employ the same blend of DDoS attacks, government website defacements, and targeted information leaks in order to delay civilian leadership decisions and influence public opinion (Korns and Kastenberg Winter 2008-2009). During the conflicts with Georgia and Ukraine, Russia was able to leverage the cyber domain to further their strategic objective of preventing the United States and NATO from deploying forces.

Outside of these strategic effects however, Russian cyber effects did little to support tactical commanders in South Ossetia. It would not be until 2014, with the invasion of Crimea that Russia would demonstrate the integration of cyber warfare at the tactical level (Sprang 2018). In one case, Russian military intelligence 'Trojan-ized' an Android app indigenously developed by a Ukrainian officer to improve the rate of fire for a specific artillery piece, the 122 mm D-30. By inserting malicious code into the legitimate app, the locational data from compromised devices could be passed to Russian forces to enable targeting of Ukrainian artillery units. According to open source assessments in 2016,

over eighty percent of Ukrainian D-30 Order of Battle (OB) had been attritted, compared to only fifty percent attrition for other types of Ukrainian artillery (Meyers 2016). While this represents a niche case, it is clear that by integrating cyber capabilities with conventional military forces, Russia has leveraged the cyber domain to create tactical advantages by exploiting the ubiquity of devices and applications in modern militaries.

Tactical effects like these are unquestionably relevant on the modern battlefield, but fundamentally are just a new mechanism to gain information advantage over the adversary. However, the cyber-attacks on the Ukrainian power system in 2015 represents a new attack vector for non-kinetic effects. In this attack, a malware known as 'Black Energy' was able to gain a foothold within the networks that supported Ukrainian regional power distribution centers (Ackerman 2017). Utilizing this foothold, the attackers were able to gain legitimate credentials and pivot to the Industrial Control Systems (ICS) that directly controlled the power distribution grid for large portions of Ukraine (SANS 2016). Subsequently, the attackers were able to manipulate breakers directly in at least 27 sub-stations across three disparate locations, effectively denying power to any customers reliant on those nodes (SANS 2016). Simultaneously, the attackers layered telephonic denial of service on the customer call center, significantly delaying the mitigation response until the power interruption was observed. In addition, malicious firmware was also uploaded to network gateway devices, denying the ability to send remote commands to the affected breakers and necessitating physical maintenance (SANS 2016). Subsequent analysis of the BlackEnergy malware has led to attribution to Russian threat actors (FBI 2016). The tempo and timing of this three-pronged attack demonstrates a robust ability to plan and execute cyber operations across a large force, against multiple independent targets, to achieve a complex, synchronized end state. Furthermore, although this particular cyber-attack occurred independent to conventional force maneuvers, such an attack against a power grid supporting adversary

Command and Control (C2) nodes represents an asymmetric operational advantage for Russia if executed at a pivotal moment in time.

In the last decade alone, Russia has demonstrated a wide range of cyber capability, from technologically unsophisticated Distributed Denial of Service (DDoS) attacks to deface government websites, to extremely advanced supply chain compromises such as the 2020 SolarWinds compromise, which gained a foothold across hundreds of US federal government systems in 2020 (Mehrotra and Sebenius 2021). These capabilities offer a wide range of advantages at every level of warfare, and US forces must base their planning assumptions potential effects to be successful. To effectively assess adversary courses of action, intelligence Airmen must be trained to understand the fundamentals of the cyber domain. These fundamentals are no more complicated than the fundamentals of electronic warfare that intelligence Airmen are required to master to support flying squadrons, but efforts are hamstrung by the false assumption that cyber is too technical without years of specialized training. Put simply, intelligence Airmen must understand how networks are structured, how they are defended, and how they are attacked if they are to be successful in a near-peer conflict. In addition, both commanders and warfighters must regularly train in contested or denied environments to develop tactics and techniques which mitigate disruptions. Currently, the majority of training in the Air Force is focused around conducting the core mission of the unit. F-16's train to conduct Suppression of Enemy Air Defenses (SEAD), F-15C's train to conduct Air Superiority, and offensive cyber operators train to conduct Offensive Cyberspace Operations (OCO). Even in the exercises nominally predicated on the integration of these dissimilar capabilities, such as Red Flag and Weapons School Integration (WSINT), cyber effects are often disconnected from the actual operational mission. This stove-piping leads to a poor understanding of the nuance of cyber warfare by non-cyber personnel, and a poor understanding of conventional force employment within the cyber community. Air Force Major Command (MAJCOM) commanders must make it clear to the 57th WG that training to and being prepared for the type of

warfare I have described in this essay is a MAJCOM interest item. After all, RED FLAG is intended to mimic a new wingman's first ten combat sorties - we cannot wish away the possibility that those sorties will be flown in a cyber degraded environment because it is inconvenient for historical desired learning objectives.

Bibliography:

Ackerman, Robert K. 2017. "Girding the Grid for Cyber Attacks." *Signal* 30-33

Bryant, William D. 2013. "Cyberspace Superiority: A Conceptual Model." *Air & Space Power Journal* 25-44.

Cunningham, Conor. 2020. *A Russian Federation Information Warfare Primer.* Research Report, Seattle: University of Washington.

DoD. 2018. *Cyber Defense Strategy.* Official Publication, Washington D.C.: Department of Defense. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

DoD. 2018. *Joint Publication 3-12 Cyberspace Operations.* Joint Doctrine Document, Washington D.C.: Department of Defense.

Duffy, Ryan. 2018. *The U.S. military combined cyber and kinetic operations to hunt down ISIS last year, general says.* May 29. Accessed January 21, 2021. https://www.cyberscoop.com/u-s-official-reveals-military-combined-cyber-kinetic-operations-hunt-isis/.

FBI. 2016. *GRIZZLY STEPPE - Russian Malicious Cyber Activity.* Joint Analysis Report, JAR-16-20296A: National Cybersecurity and Communications Integration Center.

Galeotti, Mark. 2019. *The Baltic States as Targets and Levers: The Role of the Region in Russian Strategy.* April 1. Accessed January 18, 2021. https://www.marshallcenter.org/en/publications/security-insights/baltic-states-targets-and-levers-role-region-russian-strategy-0.

Korns, Stephen, and Joshua Kastenberg. Winter 2008-2009. "Georgia's Cyber Left Hook." *Parameters* 60-76.

Meyers, Adam. 2016. "Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units." *Crowdstrike.* December 22. Accessed January 26, 20201. https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/.

Mueller, Robert S. 2019. *Report on the Investigation Into Russian Interference In the 2016 Presidential Election.* Department of Justice Report, Washington D.C.: Department of Justice.

SANS. 2016. *Analysis of the Cyber Attack on the Ukrainian Power Grid.* ICS Case Study, Washington D.C.: Electricity Information Sharing and Analysis Center.

Sprang, Ryan. 2018. "Russia in Ukraine 2013-2016: The Application of New Type Warfare Maximizing the Exploitation of Cyber, IO and Media." *Small Wars Journal.*

Tucker, Patrick. 2020. *A Big 2020 Election Hack Never Came. Here's Why.* November 4. Accessed January 26, 2021. https://www.defenseone.com/threats/2020/11/big-2020-election-hack-never-came-heres-why/169806/.

Weisgerber, Marcus. 2015. *As Russia Improves Its Surface-to-Air Missiles, US Looks to Counter.* April 8. Accessed January 26, 2021. https://www.defenseone.com/threats/2015/04/russia-improves-its-surface-air-missiles-us-looks-counter/109684/.

Williams, Brett T. 2014. "The Joint Force Commander's Guide to Cyberspace Operations." *Joint Force Quarterly* 12-19.