**Military Cyber Affairs**
**The Journal of the Military Cyber Professionals Association**
ISSN: 2378-0789

Volume 1 | Issue 1 Article 7

2015

# Brandishing the Cybered Bear: Information War and the Russia-Ukraine Conflict

Azhar Unwala
*Georgetown University*, ahu5@georgetown.edu

Shaheen Ghori
*National Defense University*, shaheenaliaghori@gmail.com

# Brandishing the Cybered Bear: Information War and the Russia-Ukraine Conflict

**Cover Page Footnote**
The authors would like to thank Dr. G. Alexander Crowther for his assistance and advice in writing this piece.

# Brandishing the Cybered Bear: Information War and the Russia-Ukraine Conflict

AZHAR UNWALA, Georgetown University
SHAHEEN GHORI, National Defense University

Russia's use of cyber power against Ukraine offered renewed insight to Russian cyber strategy and capabilities. This article dissects the Russia-Ukraine conflict by analyzing Russia's strategic doctrine, tactical maneuvers, and capabilities in the information realm. Understanding the Russia-Ukraine conflict in this manner can inform and strengthen U.S. cyber policy and strategy. In particular, U.S. strategic planners and cyber professionals should consider internalizing Russian strategic thinking regarding cyber power and promote tactical improvements in resilience, intelligence, and information among itself and its allies.

• **Cyber power** **Russia** **Ukraine** **Cyber strategy**

## INTRODUCTION

When Russian forces entered the Crimean Peninsula on March 2, 2014, they had already shut down Crimea's telecommunications infrastructure, disabled major Ukrainian websites, and jammed the mobile phones of key Ukrainian officials. Undeniably, Russia's use of cyber power was crucial in its offensive against Ukraine and its annexation of Crimea. However, realizing the extent of Russia's cyber power in this conflict requires grasping Russia's strategic and tactical maneuvers in this domain. This article analyzes Russia's cyber strategy and tactics against Ukraine in an effort to inform U.S. cyber policy. Part I surveys the strategic cyber doctrines of Russia and the United States. Part II examines a case study of Russia's cyber power against Ukraine. Drawing upon insights from the Russia-Ukraine case, Part III offers strategic and tactical recommendations that the United States should employ as well as promote among its allies.

## I. DECIPHERING DOCTRINES: RUSSIA AND THE UNITED STATES

### 3.1 RUSSIA

Understanding Russian cyber power in Ukraine requires conceptualization of Russia's strategic thinking in this area. In official and unofficial doctrine, Russia typically refers to a holistic concept of "information war," which encompasses cyber espionage, cyber attacks, and strategic communications.[1] Russia's official view of cyber power stems from its *Information Security Doctrine*, dated September 9, 2000. This document affirms a long-standing policy of state influence over the media, arguing that the government must ensure pro-Russian messaging regardless of whether media sources are state-controlled or private. Yet the *Doctrine*'s language is largely defensive, and fails to mention any Russian state role in offensive cyber capabilities.[2] The lack of state-sponsored cyber power was a characteristic of the April 2007 cyber attacks against Estonia and the 2008 Russo-Georgian War. In both cases, cyber attacks supporting Russian strategic goals were carried out by non-state hacking groups and were not positively linked to the Russian government.[3] These attacks were largely unsophisticated distributed denial-of-service (DDoS) attacks against government, media, and financial websites, and generated little lasting damage with limited payoff. Despite their tactical success in

[1] Keir Giles, "'Information Troops' – a Russian Cyber Command?" *3rd International Conference on Cyber Conflict* (2011): 46.
[2] *Information Security Doctrine of the Russian* Federation, 2008, http://archive.mid.ru//bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument.
[3] Sergei Medvedev, "Offense-Defense Theory Analysis of Russian Cyber Capability," *U.S. Nav Postgraduate School* (2015): 2-3.

Estonia, the attacks did not lead to a pro-Russian outcome.[4] Similarly, while cyber attacks initially overwhelmed Georgia's defenses, Georgians simply restored denied websites on foreign servers.[5] More importantly, these cases demonstrated strategic drawbacks to the lack of Russian state involvement in cyber attacks. First, non-state hacking groups may not possess the resources or skills for high-impact cyber attacks that manifest lasting effects.[6] Second, unsophisticated attacks can upset an adversary's decision-making by adding a scenario that the defender must react to, but those attacks require organization and precision. In Georgia's case, incoordination between hacking groups diminished the value of DDoS attacks by allowing Georgians to reconstitute their services on third party servers. The lack of coordination also produced indiscriminate attacks that included targeting Estonian and U.S. websites. This increased the assignment of blame for cyber attacks towards Russia, and may have risked escalating the conflict internationally.[7]

The insights gained from Estonia and Georgia influenced the creation of *The Military Doctrine of the Russian Federation*, approved on February 5, 2010. This doctrinal update codified reforms to transition Russia's mass-mobilization, Soviet-era military to a modern, highly mobile force. One of these reforms was the development of "forces and resources for information warfare," acknowledging that future military conflicts will include an information component. In addition to providing improved information support to Russian armed forces, the directive explains information war's function is "to achieve political objectives without the utilization of military force and, subsequently, in the interest of shaping a favorable response from the world community to the utilization of military force."[8] Further explanation of information war's functions are highlighted in the *Conceptual Views on the Activity of the Russian Federation Armed Forces in Information Space*, released on December 22, 2011. Information war, according to the *Views*, aims to damage information systems and critical infrastructure, subvert political, economic, and social systems, instigate "mass psychological work on the population to destabilise the society and state," and coerce targets to make decisions against their interests.[9] Together, these two strategic documents suggest a greater state role in conducting information war as a central component of future conflicts. They also stress information war's political functions, which in some cases may be more effective than the use of force.

Unofficial sources also expose aspects of Russia's information war strategy.[10] One authoritative source is Russian Chief of the General Staff Valery Gerasimov, who outlined necessary approaches for 21st century warfare in a 2013 article.[11] Gerasimov recognizes that future conflicts must include an information element, which can asymmetrically lower an adversary's combat potential in addition to creating "a permanently operating front through the entire territory of an enemy state…" According to Gerasimov, modern warfare should also rely on covert action, special-operations forces, and private contractors until the final stages of a conflict when success is guaranteed.

A number of implications can be drawn from the development of Russia's information war doctrine. First, the Russian state will be involved in coordinating and executing information war. These operations will largely be covert, and involve special-operations and contractor forces. Second, Russia will use information war prior to and during a conflict to understand an enemy, build support for military action, isolate the enemy informationally and internationally, and undermine the enemy's

[4] Ibid. 21.
[5] Ibid. 22-25.
[6] Max Strasser, "Why Ukraine Hasn't Sparked a Big Cyberwar, So Far," *Newsweek*, March 18, 2014, http://www.newsweek.com/why-ukraine-hasnt-sparked-big-cyberwar-so-far-232175.
[7] Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War," *Security Dialogue* 43, no. 1 (February 2012): 16-18; and Timothy L. Thomas, "The Consequences of August 2008," in *Russian Information Warfare Theory* (Strategic Studies Institute, 2010): 279-282.
[8] *The Military Doctrine of the Russian Federation*, The School of Russian and Asian Studies, 2010, http://www.sras.org/military_doctrine_russian_federation_2010.
[9] Keir Giles, "Russia's Public Stance on Cyberspace Issues," *4th International Conference on Cyber Conflict* (2012): 67-68.
[10] For a summary of unofficial sources regarding Russia's information war strategy prior to 2013, see Stephen Blank, "Russian Information Warfare as Domestic Counterinsurgency," *American Foreign Policy Interests* 35, no. 31 (2013): 34-37.
[11] Valery Gerasimov on Mark Galeotti's blog, "The 'Gerasimov Doctrine' and Russian Non-Linear War," February 27, 2013, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.


DOI: http://dx.doi.org/10.5038/2378-0789.1.1.1001

combat response. Third, information war will aim to undermine an enemy's state and societal functions, coerce adversaries, and disseminate a pro-Russian narrative of the ensuing conflict.

### 3.2 UNITED STATES

Addressing the Russian doctrine for information war also warrants an analysis of U.S. doctrine, codified in the Joint Chiefs of Staff's JP 3-12 *Cyberspace Operations* (February 2013), JP 3-13 *Information Operations* (November 2014), and most recently the Department of Defense's (DoD) *Cyber Strategy* (April 2015). According to JP 3-12, Cyberspace Operations (CO) are composed of the military, intelligence, and ordinary business operations of the DoD in and through cyberspace.[12] The DoD categorizes CO as offensive, intended to project power by the application of force; defensive, intended to defend DoD or other friendly cyberspace; or internal, taken to design, build, configure, secure, operate, and sustain DoD communications systems. Notably, the United States does not restrict its operations by classifying them as only defensive; rather it enables a full spectrum of CO for a variety of purposes. Under this document, future CO produced by the United States—such as Stuxnet—as well as defense programs, possess protocols for their use.

Information Operations (IO) guidelines are defined in Joint Publication 3-13 (November 2014) as the integrated employment, during military operations, of Information-Related Capabilities (IRCs) in concert with other lines of operation to influence, disrupt, or corrupt the decision making of adversaries and potential adversaries.[13] Through incorporating changes to this document, the Joint Chiefs of Staff are emphasizing the role information operations will have in future conflict; however, they have limited themselves to employing IO only during military operations. This might indicate that the United States believes that IO are only beneficial during military operations. A further limitation to U.S. IO is that they are used in conjunction with other lines of operation, such as cyberspace operations, public affairs, strategic communication, and key leader engagement,[14] not as their own offensive strategy.

Moreover, the Department of Defense's *Cyber Strategy* (April 2015) outlines the strategic direction that cyber operations are heading as well as evaluating the current threats that the government faces. The strategic goals are as follows:

1. Build and maintain ready forces and capabilities
2. Defend the DoD Information Network
3. Be prepared to defend the U.S. Homeland and U.S. vital interests
4. Build and maintain robust international alliances to deter shared threats and increase international security and stability[15]

The fourth goal highlights that cyber threats create security and stability issues and mentions alliances as a future focus area. It is possible that referring to allies relates to defending against cyber attacks against key NATO allies and Major Non-NATO Allies (MNNAs). The United States also realizes the need for cyber cooperation so that weaker states cannot be held prey when targeted by cyber attacks. By publishing this document, the United States acknowledges the current deficiencies in addressing cyber threats while formulating plans to solve them over the next five years.

Several implications can be drawn from the United States' doctrines of information war. First, the United States views cyberspace as a critical area to improve over the next couple of years. Funds, manpower, and attention are all shifting to strengthen America's position in this developing field. Second, while IO are achieving more focus, they are limited in their employment due to the guidelines set forth in JP 3-12. Finally, the U.S. doctrines are reactionary and living, changing whenever new events take place and projecting ambiguity when dealing with developing problems. In the case of the Russia-Ukraine conflict, the United States did not have a strong response to Russian cyber assaults on Ukraine.

---

[12] "Cyberspace Operations," Joint Publication 3-12, *U.S. Department of the Army,* February 5, 2013, www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

[13] "Information Operations," Joint Publication 3-13, *U.S. Department of the Army,* Originally published November 2012, updated November 27, 2014, www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.

[14] Ibid.

[15] *The Department of Defense Cyber Strategy,* April 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

## II. EXAMINING THE RUSSIA-UKRAINE CONFLICT

The 2014 Russia-Ukraine conflict offers a valuable case study of Russia's information war strategy. It is important to note that Russia initiated offensive cyber operations against Ukraine as early as 2009 as a part of a broader information war campaign against NATO and EU countries.[16] It was only in March 2014 that information war operations intensified against Ukraine. In that month, the Russian parliament authorized military force in Ukraine, President Vladimir Putin signed legislation incorporating Crimea into the Russian Federation, and Russian military forces amassed along the Ukrainian national border.[17] The following section outlines the three pillars of Russia's information war campaign against Ukraine: cyber espionage, cyber attacks, and strategic communications.

### 3.1 ESPIONAGE

Russia's espionage efforts relied upon standard open-source information collection,[18] as well as interception of Ukrainian telecommunications infrastructure and targeted cyber operations. Intercepting Ukrainian telecommunications infrastructure was logical for Russia. First, most Ukrainian telecommunications systems rely on Russia for manufacturing or maintenance of the technology. In fact, the most common backdoor into Ukrainian systems utilized by the Ukrainian government for surveillance was modeled after the Russian KGB intercept system. Second, Russian mobile telecommunications firms such as Vimpelcom and MTS held a considerable portion of the Ukrainian market; MTS held the second largest market share in September 2013.[19] Since it is widely suspected that the Russian government collaborates with private companies, it is safe to assume that the Russian government possessed ownership insight into most Ukrainian telecommunications infrastructure.[20] This is evident by the text messages many participants of an anti-Russian demonstration in Kiev received, reading, "Dear subscriber, you are registered as a participant in a mass disturbance."[21]

Russia also employed cyber espionage operations targeting the computers and networks of journalists in Ukraine, as well as Ukrainian, NATO, and EU officials. Some operations were already underway well before the conflict began. The Sandworm espionage operation, which exploited a previously unknown Windows vulnerability, had started as early as 2009 and targeted EU and NATO telecommunications infrastructure through 2014. Sandworm's malware had intensified and targeted Ukrainian government networks during September 2014, which coincided with the NATO summit in Wales.[22] Other espionage operations began closer to the conflict. Operation Armageddon began in mid-2013 to target Ukrainian government, law enforcement, and military officials. This occurred just as Ukraine and the EU commenced active negotiations for an Association Agreement, which Russia publicly deemed a national security threat.[23] As anti-government protests began in Ukraine, an advanced malware named 'Snake' infected the Ukrainian prime minister's office and several embassies outside the country.[24] Furthermore, Operation Potao began as Russia commenced its invasion of Crimea, targeting computers and mobile communications of Ukrainian officials and news agencies.[25]

---

[16] "Russian Cyber Espionage Campaign – Sandworm Team," *iSight Partners* (2014): 1-11.
[17] Kenneth Geers, "Strategic Analysis: As Russia-Ukraine Conflict Continues, Malware Activity Rises," *FireEye Blogs* (2014): https://www.fireeye.com/blog/threat-research/2014/05/strategic-analysis-as-russia-ukraine-conflict-continues-malware-activity-rises.html.
[18] "Ukraine: Russia's New Art of War," *Financial Times*, August 28, 2014, http://www.ft.com/cms/s/0/ea5e82fa-2e0c-11e4-b760-00144feabdc0.html.
[19] Patrick Tucker, "Why Ukraine Has Already Lost The Cyberwar, Too," *Defense One* (April 2014): http://www.defenseone.com/technology/2014/04/why-ukraine-has-already-lost-cyberwar-too/83350/.
[20] Ibid; and "Ukraine: Russia's New Art of War."
[21] Ibid.
[22] "Russian Cyber Espionage Campaign – Sandworm Team."
[23] "Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare," *LookingGlass Cyber Threat Intelligence Group* (April 2015): 3-9.
[24] David E. Sanger and Steven Erlanger, "Suspicion Falls on Russia as 'Snake' Cyberattacks Target Ukraine's Government," *New York Times,* March 8, 2014, http://www.nytimes.com/2014/03/09/world/europe/suspicion-falls-on-russia-as-snake-cyberattacks-target-ukraines-government.html.
[25] Robert Lipovsky and Anton Cherepanov, "Operation Potao Express," *ESET Report* (July 2015): 9-13.

The timing and construction of these espionage operations indicated Russian state involvement, particularly by the Russian Federal Security Service (FSB).[26] In many cases, the deployed malware was consistently updated in a formal code development environment with Russian time and language settings.[27] Malware was also tailored towards specific, high-level targets for use in spear-phishing and whaling operations.[28] Most espionage malware payloads consisted of Microsoft Office or Adobe files that held seemingly legitimate reports regarding EU strategic competiveness and energy, lists of Russian sympathizers and "terrorist" actors, and briefings of recent developments in the Ukraine conflict.[29] Even operations targeting journalists held lures regarding publication opportunities.[30] In Operation Potao's case, the payloads included a modified encryption service containing a backdoor for Russian access.[31] The operations were also constructed to avoid discovery and attribution; the malware often contained unused machine instructions, obfuscated strings, and counter-analysis capabilities.[32] In the case of 'Snake', the malware garnered full remote access to a compromised system while blending in with network traffic to avoid detection.[33]

Russia's advanced espionage techniques provided the Kremlin with insight to Ukrainian, EU and NATO strategic intentions to support Russian strategy. They also enabled Russia to monitor Ukraine's strategic thinking in real time. Furthermore, targeting journalists permitted Russia to monitor public opinion, identify dissidents, and create avenues to spread disinformation and pro-Russian messaging.[34]

## 3.2 CYBER ATTACKS

A number of cyber attacks intending to disrupt or destroy targets were carried out in Ukraine. Like the Estonia and Georgia cases, pro-Russian, non-state hacking groups performed a variety of cyber attacks. One group based in Ukraine called Cyber Berkut was especially prominent. Cyber Berkut executed DDoS attacks and defacements against Ukrainian and NATO webpages,[35] intercepted U.S.-Ukrainian military cooperation documents,[36] and attempted to influence the Ukrainian parliamentary elections by disrupting Ukraine's Central Election Commission network.[37] While it is possible that the Russian government supported these groups clandestinely, the unsophisticated and indiscriminate nature of attacks indicates minimal coordination or cooperation with the Kremlin.[38] Additionally, just as Estonia and Georgia demonstrated, these non-state attackers generated nominal damage. That is not to say their strategic role was irrelevant; it is likely that these hacking groups fomented confusion

[26] Robert Hackett, "Russian cyberwar advances military interests in Ukraine, report says," *Fortune*, April 29, 2015, http://fortune.com/2015/04/29/russian-cyberwar-ukraine/; and Jen Weedon and Laura Galante, "Intelligence Analysts Dissect the Headlines: Russia, Hackers, Cyberwar! Not So Fast." *FireEye Blogs*, March 12, 2014, https://www.fireeye.com/blog/executive-perspective/2014/03/intel-analysts-dissect-the-headlines-russia-hackers-cyberwar-not-so-fast.html.
[27] "APT 28: A Window Into Russia's Cyber Espionage Operations?" *FireEye Special Report*, (2014): 24.
[28] Ibid. 6, 20.
[29] Aarti Shahani, "Report: To Aid Combat, Russia Wages Cyberwar against Ukraine," *NPR*, April 28, 2015, http://www.npr.org/sections/alltechconsidered/2015/04/28/402678116/report-to-aid-combat-russia-wages-cyberwar-against-ukraine.
[30] "APT28," (2014): 9-12.
[31] Robert Lipovsky and Anton Cherepanov 2015: 14.
[32] Ibid. 5.
[33] Tim Maurer and Scott Janz, "The Russia-Ukraine Conflict: Cyber and Information Warfare in a Regional Context," *The International Relations and Security Network*, October 17, 2014, http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=184345.
[34] "APT28," (2014): 10-11.
[35] Petro Zamakis, "Cyber Wars: The Invisible Front," *Ukraine Investigation*, April 24, 2014, http://ukraineinvestigation.com/cyber-wars-invisible-front/.
[36] CyberBerkut, http://cyber-berkut.org/en/.
[37] "Hackers Target Ukraine's Election Website," *Agence France-Presse*, October 25, 2014, http://www.securityweek.com/hackers-target-ukraines-election-website.
[38] Jen Weedon and Laura Galante, "Intelligence Analysts Dissect the Headlines: Russia, Hackers, Cyberwar! Not So Fast." FireEye Blogs, March 12, 2014, https://www.fireeye.com/blog/executive-perspective/2014/03/intel-analysts-dissect-the-headlines-russia-hackers-cyberwar-not-so-fast.html.

and disarray among their targets,[39] undermined the Ukrainian state's credibility among its people,[40] and intimidated Ukraine's allies.[41]

Additionally, a variety of cyber attacks can be linked to the Russian government. On February 28, 2014, shortly after then-President Victor Yanukovych fled Ukraine, armed Russian soldiers bearing no insignia took over the Simferopol International Airport, the Crimean Peninsula's main airport.[42] Similar unmarked soldiers took over a Ukrtelecom building in Sevastopol, a city in southwestern Crimea.[43] Ukrtelecom, Ukraine's National Telecommunications operator, subsequently issued a report claiming that the soldiers "seized several communications hubs in Crimea," tampered with Crimean fiber optic cables, and damaged its optical fiber and conductor units.[44] The Russian soldiers also equipped the remaining active fiber optic cables with data intercept devices.[45]

The logic behind these events can be explained by understanding Ukraine's telecommunications geography. Ukraine's Internet Service Providers (ISPs) were decentralized and held terrestrial and satellite path diversity to the rest of the world.[46] This system differed from Georgia's, which could only access the Internet by traversing Russian and Turkish infrastructure.[47] As a result, isolating Ukraine from telecommunications was slightly more difficult as it required Russian forces to target key cyber terrain at operationally decisive points. Luckily for Russia, Crimea was one of the vulnerable areas in Ukraine since it only held one Internet Exchange Point (IXP) that connected the peninsula to the rest of the country. If Crimea's IXP were damaged or shut down, Crimea would be completely isolated, allowing Russia to control the region's communications.[48] Furthermore, hampered communications services would short-circuit Ukraine's crucial support services from assisting Crimea in the event of a conflict with Russia. Military operations in addition to first-aid, fire and rescue services would be unable to provide relief to the region, forcing the Crimean people to rely on Russia.[49] Furthermore, Russia would monitor any residual communications in or out of Crimea, providing them with precise intelligence on Crimea's interactions with the rest of Ukraine.

Russia's logic proved successful. Once Crimea was completely isolated, Russian troops entered the region with little difficulty on March 2.[50] Immediately afterwards, multiple Ukrainian government, news, and social media websites were shut down and the mobile phones of Ukrainian officials and parliament members were hacked or blocked for the next three days.[51] Given the timeliness of these attacks, it is possible that Russian Military Intelligence (GRU) directed them.[52] Combined with attacks on Crimean telecommunications prior to Russia's invasion, the post-invasion cyber attacks significantly lowered the response potential of the Ukrainian government. First, Ukrainian officials were unable to communicate with Crimean sources on the ground to acquire an

[39] Tim Maurer and Scott Janz 2014.
[40] Mark Clayton, "Ukraine election narrowly avoided 'wanton destruction' from hackers," *Christian Science Monitor*, June 17, 2014, http://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers-video.
[41] Max Cherney, "Pro-Russian Hackers Took Down Three NATO Websites," *Motherboard*, March 16, 2014, http://motherboard.vice.com/blog/pro-russia-ukranians-hack-nato-websites; and Thomas Barrabi, "NATO Not Responsible For Ukraine's Security From Russia, Should Focus On Member Nations, Latvian Envoy Says," *International Business Times*, May 6, 2015, http://www.ibtimes.com/nato-not-responsible-ukraines-security-russia-should-focus-member-nations-latvian-1910551.
[42] "Feb. 28 Updates on the Crisis in Ukraine," *The New York Times: The Lede*, February 28, 2014, http://thelede.blogs.nytimes.com/2014/02/28/latest-updates-tensions-in-ukraine/.
[43] Ibid.
[44] Ibid.
[45] "The Ukrainian Crisis – A Cyber Warfare Battlefield," *Defense Update*, April 5, 2014, http://defense-update.com/20140405_ukrainian-crisis-cyber-warfare-battlefield.html.
[46] Sanja Kelly et al., "Freedom on the Net 2014," *Freedom on the Net* (Freedom House, 2014): 820-1.
[47] John Markoff, "Web becomes a battleground in Russia-Georgia conflict," *The New York Times,* August 12, 2008, http://www.nytimes.com/2008/08/12/world/europe/12iht-cyber.4.15218251.html.
[48] Jason Rivera, "Has Russia Begun Offensive Cyberspace Operations in Crimea?" *Georgetown Security Studies Review*, March 2, 2014, http://georgetownsecuritystudiesreview.org/2014/03/02/has-russia-begun-offensive-cyberspace-operations-in-crimea/.
[49] "Feb. 28 Updates on the Crisis in Ukraine."
[50] Tim Maurer and Scott Janz 2014.
[51] Ibid.
[52] "The Ukrainian Crisis – A Cyber Warfare Battlefield." *Defense Update* 2014.

accurate understanding of the ensuing conflict. Second, Ukrainian officials were unable to share information or execute command and control processes among themselves. Third, Ukrainian officials were unable to communicate with foreign allies, placate pro-Russian Ukrainians, or make efforts to undermine Moscow.[53] In this way, Russian strategic planners were able to operate several steps ahead of their Ukrainian counterparts during the conflict.

### 3.3 STRATEGIC COMMUNICATIONS

A central component of Russia's information war on Ukraine was the body of online communications disseminated by Russian officials, journalists, and media sources to promote a pro-Russian view of the conflict. This strategy is an extension of Russia's domestic media policies. The Internet is one of the few remaining avenues to express popular dissent within Russia, since television is almost exclusively state-controlled and a common outlet for the Putin administration.[54] As a result, the Russian government invests heavily in analyzing and influencing online media pipelines.[55] Against Ukraine, Russia supported journalists, bloggers, and individuals within social media networks to broadcast pro-Russian narratives.[56] In one case, Russia paid a single person to hold multiple different web identities. One actor in St. Petersburg conveyed that she was acting as three different bloggers with ten blogs, while also commenting on other sites.[57] Another individual was employed to simply comment on news and social media 126 times every twelve hours.[58] Interestingly, pro-Russian online media also mimicked anti-Russian sources. The website *Ukrainskaya Pravda* was a pro-Russian version of the popular Ukrainian news site *Ukrains'ka Pravda*. These pro-Russian sources would communicate false narratives about actual events, such as denying the presence of Russian military in Ukraine[59] or blaming the West for conducting extensive information war against Russia.[60] Another example is the dissemination of images depicting columns of refugees fleeing Ukraine to Russia, when in reality they were daily traffic between Ukraine and Poland.[61] Along these lines, a pro-Russian web presence misled Ukrainian citizens, journalists, and other onlookers to the conflict seeking reliable sources of information.[62]

Russia's strategic communications also alienated Ukraine from its allies. This relied upon the dissemination of doctored images. For example, pro-Russian media sources would spread photos of Ukrainian tanks, flags, and soldiers altered to bear Nazi symbols in an effort to associate the Ukrainian government with resurgent Nazism. These tactics were especially provocative as some European countries like Germany are revolted by their Nazi history and were likely to distance themselves from Ukraine.[63] In other cases, hacking groups leaked privileged information, such as the controversial telephone conversation between U.S. Assistant Secretary of State Victoria Nuland and U.S. Ambassador to Ukraine Geoffrey Pyatt, which may have embarrassed the United States.[64]

---

[53] Weedon and Galante 2014.

[54] Sacha Dov Bachmann and Hakan Gunneriusson, "Russia's Hybrid Warfare in the East: The Integral Nature of the Information Sphere," *Georgetown Journal of International Affairs: International Engagement on Cyber* V (2015): 199-200.

[55] "Russia Update: Defense Ministry Plans New Computer Programs to Monitor, Analyze Social Media," *The Intepreter Magazine*, January 29, 2015, http://www.interpretermag.com/russia-update- january-29-2015.

[56] Jill Dougherty, "Everyone Lies: The Ukraine Conflict and Russia's Media Transformation," *Discussion Paper Series*, Shorenstein Center on Media, Politics, and Public Policy (July 2014): 2-29.

[57] Sacha Dov Bachmann and Hakan Gunneriusson 2015: 200.

[58] Ibid.

[59] Ibid.

[60] "'Ukraine, West wage information war against us' – Russians" *Russia Today*, November 12, 2014, http://www.rt.com/politics/204827-ukraine-west-information-warfare.

[61] Peter Pomerantsev, "Can Ukraine Win Its Information War With Russia?" *The Atlantic*, June 11, 2014, http://www.theatlantic.com/international/archive/2014/06/can-ukraine-win-its-information-war-with-russia/372564.

[62] Petro Zamakis 2014.

[63] James J. Coyle, "Russian Disinformation Alienates the West from Russian Periphery," *Atlantic Council*, 2015, http://www.atlanticcouncil.org/blogs/new-atlanticist/russian-disinformation-alienates-the-west-from-russian-periphery?tmpl=component&print=1.

[64] Daisy Sindelar, "Brussels, Kyiv, Moscow React to Leaked Nuland Phone Call," *Radio Free Europe/Radio Liberty*, February 7, 2014, sec. Ukraine, http://www.rferl.org/content/nuland-russia-eu- ukraine-reaction/25256828.html; and Tim Maurer and Scott Janz 2014.

Russia also utilized television to generate support for intervention in Crimea. Here, the narrative was that Moscow must invade Crimea to protect native Russian speakers from danger.[65] State-backed outlets such as RT and Channel One frequently presented violent, suspense-filled coverage of the Ukraine conflict. A notable excerpt of this coverage was of a crying woman describing Ukrainian soldiers crucifying a baby and killing his mother.[66] This story was false,[67] as were numerous stories broadcasted across Russian television. Just as a single individual would operate multiple online personas, particular individuals would espouse multiple television personas purporting false anecdotes. Across multiple TV channels, the same weeping women and injured men would be identified as "a soldier's mother," then an "Odessa resident," and then an "anti-Maidan activist," all recounting different injustices they faced against the Ukrainian state.[68] This tactic was especially useful after Russia's unmarked troops isolated Crimea's communications infrastructure. Ukrainian channels were subsequently taken off the air and replaced with Russian state channels, which enabled pro-Russian activists in the region to gain legitimacy against the Ukrainian state.[69]

A final component of Russia's strategic communications strategy was denying official Russian involvement in attacks until the later stages of the conflict.[70] Drawing upon the disinformation advanced by Russian media, Moscow's denial prevented a quick response from the West.[71] At the same time, Moscow constantly communicated the necessity of de-escalating the conflict, which obscured its strategy to NATO and the EU.[72] In this manner, Russia leveraged its strategic communications to operate within Western decision-making and reduce the costs of its actions against Ukraine.[73] Once President Putin admitted the presence of Russian troops in Ukraine, he had already completed Crimea's annexation.[74]

## III. ANALYSIS AND RECOMMENDATIONS

Russia's success against Ukraine demonstrates the value of doctrinal improvements to its information war strategy after the Estonia and Georgia conflicts. A couple of broad strategic insights can be gained by analyzing Russia's information war tactics in this case. First, the role of state-led, covert cyber offensives was crucial in penetrating Ukrainian state apparatuses to achieve intelligence from high-value targets, as well as disabling key portions of Ukrainian cyber terrain to augment Russia's ground objectives. While non-state hacking groups assisted Russia in fomenting disarray within Ukrainian decision-making and response apparatuses, they alone were insufficient in achieving Russia's objective of annexing Crimea. Second, components of Russia's information war operated synergistically to continuously support Moscow's advantage in the conflict. Intelligence acquired from

---

[65] Colin Daileda, "Could Russia Use Cyberwarfare to Further Destabilize Ukraine?" *Mashable*, April 4, 2014, http://mashable.com/2014/04/14/russia-ukraine-cyber-warfare/.

[66] Arcady Ostrovsky, "The crucifixion of a 3-year old, the U.S. helped Kiev shoot down Flight 17, and other tales the Kremlin media tell," *StopFake.org*, July 31, 2014, http://www.stopfake.org/en/the-crucifixion-of-a-3-year-old-the-u-s-helped-kiev-shoot-down-flight-17-and-other-tales-the-kremlin-media-tell/.

[67] Ibid.

[68] Peter Pomerantsev, "Inside the Kremlin's hall of mirrors," *The Guardian*, April 9, 2015, http://www.theguardian.com/news/2015/apr/09/kremlin-hall-of-mirrors-military-information-psychology.

[69] Arcady Ostrovsky 2014.

[70] Yuras Karmanau and Vladimir Isachenkov, "Vladimir Putin admits for first time Russian troops took over Crimea, refuses to rule out intervention in Donetsk," April 17, 2014, *National Post*, http://news.nationalpost.com/news/world/vladimir-putin-admits-for-first-time-russian-troops-took-over-crimea-refuses-to-rule-out-intervention-in-donetsk.

[71] Douglas Mastriano et. al, "Analysis of Russian Strategy in Eastern Europe, an Appropriate U.S. Response, and the Implications for U.S. Landpower," *Project 1704*, U.S. Army War College (2015): 6-8.

[72] Ibid; and Sacha Dov Bachmann and Hakan Gunneriusson 2015.

[73] Ibid.

[74] Ibid; and Yuras Karmanau and Vladimir Isachenkov 2014.

cyber espionage supported Russia's cyber attacks and strategic communications. Cyber attacks disabled Ukraine's ability to counter Russian strategic communications and cyber espionage. Strategic communications undermined the legitimacy of the Ukrainian state to its citizens and allies, enabling Russian cyber attacks and espionage to succeed without robust responses from Ukrainian society and its foreign partners.[75] Third, Russia demonstrated the potential of applying information war concepts to kinetic war tactics. The problem of identifying Russia's unmarked soldiers in Crimea mirrored the difficulties in attributing cyber operations to a particular actor. In both cases, concealment of identity lowered the costs of Russia's actions–there was little to no kinetic response to Russia's kinetic operation. This kinetic operation also possessed objectives in the cyber realm. By using land forces to damage communications and isolate Crimea, Russia demonstrated further synergistic possibilities between the cyber and physical domains.

It is possible that this synergistic potential of warfare is only realized through Russia's holistic conceptualization of "information war," rather than the U.S. categorization of cyberspace operations versus information operations, military information versus non-military information, and offensive capabilities versus defensive capabilities. For the United States, the "information war" concept is divided up into different doctrines and policies as if it were another physical domain of war. On the other hand, those distinctions and divisions are largely irrelevant for Russia. As the Ukraine conflict demonstrates, the information battlefield exists everywhere. The distinctions between combatant and non-combatant are blurred as civilians are targeted and utilized as part of broader information campaigns to support Russian strategic military goals. Moreover, traditional conceptions of offense and defense are erased as attacks on key Ukrainian cyber terrain enable Russia to defend itself by denying possible Ukrainian escalatory responses.[76] Along these lines, the United States must internalize these strategic concepts to prepare itself for similar dynamic, synergistic, and hybrid conflicts involving the information sphere.

In a similar vein, the United States must improve its efforts to defend and counter Russian information war tactics. In light of Russia's maneuvers against Ukraine, the United States should promote improvements in resilience, intelligence, and information among itself and its allies.

### 3.1 RESILIENCE

Russia's success was partly attributed to Ukraine's inability to defend itself or adequately respond to Russian cyber attacks. While Ukrainian hacker groups did respond to Russia's cyber offensives, these attacks were often website defacements or denial or service, and contributed little to preventing Russia's annexation of Crimea.[77] Furthermore, Ukraine—and Crimea, especially—had no way to counter Russia's cyber operations once their systems were shut down. This was due to growing vulnerabilities in Ukraine's cyber defense architecture,[78] as well as the geography of its telecommunications infrastructure. One IXP for the entirety of Crimea allowed Russia to extinguish all online and mobile communications, rendering the region completely vulnerable.

In order to prevent this effect, the United States should promote a policy of structural diversification of key telecommunications nodes and exchange points. With U.S. guidance, Ukraine can develop its Internet infrastructure by opening up multiple IXPs for its regions to prevent susceptibility of physical damage to telecommunications and isolation from the rest of the country. Opening up additional IXPs carries additional benefits besides maintaining security, such as cost, latency, and bandwidth.[79] Increasing the bandwidth passing through an exchange will allow Ukraine to reduce the damage caused by DDoS attacks, since the provider would be able to handle and process more Internet traffic.

---

[75] Sacha Dov Bachmann and Hakan Gunneriusson 2015: 200-206.
[76] Nikola Schmidt, "Neither Conventional War, nor a Cyber War, but a Long-Lasting and Silent Hybrid War," *Defense and Strategy* 14, no. 2 (2014): 80-85.
[77] Petro Zamakis 2014.
[78] Ibid.
[79] "Global Internet Exchange Points," *The Border Gateway Protocol Advanced Internet Routing Resources*, http://www.bgp4.as/internet-exchanges.

Another way to sustain resilience from a DDoS attack is to pay networking companies to allocate more bandwidth through Internet providers.[80] The United States can aid Ukraine and other allies in the future by filtering unnecessary Internet traffic so that businesses in the host country can continue their operations. The United States successfully mitigated a DDoS campaign against its banks in 2012 by maintaining tight control of their networks[81] and redirecting unauthorized traffic to other servers. An international effort can also be taken to help break down botnets that aid in DDoS operations. Soliciting private companies to monitor traffic traveling through IXPs will help attribute the bots used in these attacks. In the case of the DDoS attack against U.S. banks, the United States government appealed to more than 100 countries to choke off debilitating computer traffic nodes around the world.[82]

Additionally, one major issue for Ukraine is its dependence on Russia for manufacturing and maintenance of its telecommunications systems. Obtaining this technology from Russia generates supply chain vulnerabilities planted by Russian corporations on behalf of Moscow. Along these lines, the United States should assist Ukraine in finding alternative sources for its telecommunications infrastructure that are trustworthy, less susceptible to Russian tampering, and contain built-in security measures.

### 3.2 INTELLIGENCE

Another aspect of Russia's success was Ukraine's inability to proactively detect and defend itself from the onslaught of Russian state and non-state cyber attacks. As a result, more robust intelligence cooperation on cyber intelligence and research is warranted. For cyber incidents that were committed by non-state groups, the United States and its allies need to rely upon intelligence to predict future cyber attacks. Most cyber criminal organizations coordinate and plan their cyber offensives through messaging boards.[83] Tracking messaging boards for Russian cyber group activity may provide valuable insight as to what websites, systems, and infrastructure will be attacked prior to the operation itself.

An added measure to confuse or delay cyber criminals is to modify the communications technology that criminals compromise. In his latest testimony, Admiral Rogers, director of USCYBERCOM, spoke of new cyber detection technologies that can relay false information to cyber attackers in order to impede their objectives.[84] This program or hardware can be shared to protect allies' systems from both cyber criminal groups and state-sponsored attacks.

### 3.3 INFORMATION

Strategic communications and information operations played a critical role in U.S. and Russian strategies during the Cold War, yet the vigor of these campaigns was lost after the conflict abated. Russia's maneuvers in Ukraine were still reminiscent of its operational deception tactics–*maskirovka*—during the Cold War.[85] The United States continues to devote resources to information operations, adapting to the advent of social media. In 2011, U.S. Central Command contracted a California corporation to develop what is described as an "online persona management service" that allows one U.S. serviceman or woman to control up to ten separate identities based all over the

---

[80] Jason Healey, "How to Beat a Russian Cyber Assault on Ukraine," March 3, 2014, *The Atlantic Council:* http://www.atlanticcouncil.org/blogs/new-atlanticist/how-to-beat-a-russian-cyber-assault-on-ukraine.

[81] Dan Holden and Curt Wilson, "Lessons Learned from the U.S. financial services DDoS Attacks," *Arbor Threat Intelligence*, December 13, 2012, https://asert.arbornetworks.com/lessons-learned-from-the-u-s-financial-services-ddos-attacks/.

[82] Ellen Nakashima, "U.S. rallied multinational response to 2012 cyberattack on American banks," *The Washington Post,* April 11, 2014, https://www.washingtonpost.com/world/national-security/us-rallied-multi-nation-response-to-2012-cyberattack-on-american-banks/2014/04/11/7c1fbb12-b45c-11e3-8cb6-284052554d74_story.html.

[83] Noa Bar-Yosef, "A Look Inside the Bustling Cybercrime Marketplace," *Security Week*, March 1, 2011, http://www.securityweek.com/look-inside-bustling-cybercrime-marketplace.

[84] Michael S. Rogers, "Statement of Admiral Michael S. Rogers," *Testimony Before the Senate Committee on Armed Services*, March 19, 2015: http://www.armed-services.senate.gov/imo/media/doc/Rogers_03-19-15.pdf.

[85] Jason Healey, "Russia vs. Ukraine: The Cyber Front Unfolds," *The Atlantic Council*, April 2, 2014, http://www.atlanticcouncil.org/blogs/new-atlanticist/russia-vs-ukraine-the-cyber-front-unfolds.


DOI: http://dx.doi.org/10.5038/2378-0789.1.1.1001

world.[86] The goal of this contract was to manipulate these fake online personas to influence Internet conversations and spread pro-American propaganda.[87] Another limited U.S. counter-effort came from the Broadcasting Board of Governors, a federal agency overseeing the Voice of America and similar radio stations aimed at the Middle East, Cuba, and Asia, who urged Baltic States to put together broadcasts to draw away from Russian television.[88] The states at most risk are Latvia, Lithuania, and Estonia, who get the majority of their news from Russian sources. The United States attempted to create a news network of free information for those nations, but it drew few viewers.[89]

In 2014, the United States Senate's Foreign Relations Committee passed the so-called "Russian Aggression Prevention Bill" that authorized $10 million a year to be used to counter Russian propaganda in Ukraine, Georgia, and Moldova by financing Voice of America and Radio Free Europe.[90] These amounts are separate from other branches of U.S. government spending like the $100 million provided by the government to NGOs in Russia and $25 million to opposition bloggers.[91] However, this fails to impress against the $500 million a year budget that Russia Today receives to broadcast its services all around the world in support of the Russian government.[92]

With Russia wielding an extensive psychological warfare capability, the United States government should reignite its information campaign to counter the attacks made by its adversaries. This could even include bringing back the U.S. Information Agency, which was disbanded and absorbed into the State Department in 1999.[93] Russia has an extremely adept propaganda machine producing and updating articles consistently as new events occur. The key to a successful U.S. campaign is a rapid reaction strategy aiming to build information-based deterrence. The United States ought to broadcast accurate sources showing enemy intent and preparations for attack as well as portray friendly intent and allied military prowess. Almost immediately after a Russian article is posted, the United States should respond by presenting elements of the true situation and turning the false information against its adversaries.[94] This has been happening on a small scale, with the U.S. government reaching out to Sony, the New York Times, and other media outlets to help tackle Russian propaganda, but these actions are sometimes inconsistent and ad-hoc. A clear and consistent policy aimed at information-based deterrence would improve the ability of the United States and its allies in countering Russian strategic communications.

## CONCLUSION

The 2014 Russia-Ukraine conflict offered fresh insight to Russia's cyber strategies and capabilities. It also exposed potential areas where U.S. cyber policy can be strengthened. While analysis and prescriptions regarding conventional military force arrangements are beyond the scope of this article, understanding cyber power's role for Russia and the United States is valuable in informing strategic planners and professionals about future cybered conflicts. In light of Russia's maneuvers against Ukraine, the United States should promote improvements in resilience, intelligence, and information among itself and its allies.

---

[86] Nick Fielding and Ian Cobain, "Revealed: U.S. Spy Operation that Manipulates Social Media," *The Guardian,* March 17, 2011, http://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks.

[87] Ibid.

[88] Chris McGreal, "Vladimir Putin's 'misinformation' offensive prompts US to deploy its cold war propaganda tools," *The Guardian*, April 25, 2015, http://www.theguardian.com/world/2015/apr/25/us-set-to-revive-propaganda-war-as-putin-pr-machine-undermines-baltic-states.

[89] Ibid.

[90] Alexander Nekrassov, "West v Russia: Propaganda war rages on," *Al Jazeera,* September 25, 2014, http://www.aljazeera.com/indepth/opinion/2014/09/west-v-russia-propaganda-war-r-20149211230376039 40.html.

[91] Ibid.

[92] Ibid.

[93] *The United States Information Agency - A Commemoration*, http://dosfan.lib.uic.edu/usia/abtusia/commins.pdf.

[94] Brian Nichiporuk, "U.S. Military Opportunities: Information-Warfare Concepts of Operation," in *Strategic Appraisal: The Changing Role of Information in Warfare*, (Rand Corporation: 1999) 193-198; and Mark Galeotti, "'The West is too Paranoid about Russia's Information War,'" *The Guardian*, July 7, 2015, http://www.theguardian.com/world/2015/jul/07/russia-propaganda-europe-america.