CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Russian Cyber-Operations in Ukraine and the Implications for NATO

by Alexander Salt and Maya Sobchuk

August 2021

POLICY PERSPECTIVE

RUSSIAN CYBER-OPERATIONS IN UKRAINE AND THE IMPLICATIONS FOR NATO

by Alexander Salt and Maya Sobchuk

August 2021

CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Prepared for the Canadian Global Affairs Institute
1800, 150 – 9th Avenue S.W., Calgary, AB T2P 3H9
www.cgai.ca

ISBN: 978-1-77397-208-4

All members of the North Atlantic Treaty Organization (NATO) should view Russia's 2014 invasion of Eastern Ukraine as a significant security issue. Although the strategic situation in Ukraine is indeed plagued by conventional combat (particularly in the Donbas region), it is important to note that Russian cyber-operations have emerged as one of the more troublesome challenges. Cyber-attacks are increasing in regularity and will likely remain a consistent part of emerging conflicts in the contemporary global security environment. Russian boldness in this context is particularly noticeable as it was just recently that Ukraine became a NATO Enhanced Opportunities Partner, meaning Russia is clearly willing to challenge the West more directly. In some ways this is not entirely a new threat. For example, Keir Giles, a Chatham House Russian security expert, has argued that Russia is essentially taking the information/propaganda experiences that it honed and mastered during the Cold War and is enhancing them by using modern information technology to amplify their effectiveness.[1] This crisis's lingering implications for the Alliance suggest it is in NATO's best interest to continue to strengthen its existing cyber-capabilities and aid Ukraine. Indeed, NATO members are best suited to respond to the broadening cyber-challenge via the Alliance framework, rather than individually, due to the inherent complexity and transnational character of cyber-threats.

Russian Cyber-Operations in Ukraine

The Russian military strategy to destabilize Ukraine involves the use of conventional ground forces and local proxies, supported by a series of ongoing cyber-attacks. These Russian cyber-operations are disrupting Ukrainian digital infrastructure, disseminating pro-Russian propaganda to break the will of the Ukrainian political elites and civilians, and trying to dissuade Ukrainian allies from further intervening. Russian hackers have co-ordinated a series of denial of service (DDoS) attacks on Ukrainian governmental websites; in particular, these hackers targeted politicians considered to hold anti-Russian views and websites relating to elections. Further, Russian hackers and bot farms are aggressively flooding various Ukrainian social media platforms with pro-Russian propaganda and fake news.[2]

Russia's cyber-operations are even influencing tactical level combat at the front lines. The Russians were able to use information technology to uncover the cellphone numbers of Ukrainian military personnel (as well as the soldiers' families) and send them a series of text messages to get them to abandon their duty. The majority of military-age personnel (18-49) have cellphones, and this allows the Russians to essentially bypass any broader defences that a military may have against enemy propaganda by sending it directly to the pockets of these young men and women.[3]

[1] Keir Giles, "Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power," Chatham House, March 2016, https://www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf.
[2] Michael Kofman, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva and Jenny Oberholtzer, *Lessons from Russia's Operations in Crimea and Eastern Ukraine* (Santa Moncia: RAND Corporation, 2017)
[3]Lucas Scarasso, "Text Messages from Hell: Restraint and Information Warfare," Modern War Institute, April 21, 2020, https://mwi.usma.edu/text-messages-hell-restraint-information-warfare/.

The Russian cyber-campaign also exemplifies the problem of attribution. The Russian government does not acknowledge nor take credit for individual cyber-attacks. This is done purposely for the presumption of deniability. However, there is also a blurred line between state and non-state actors in this process as various pro-Russian hacker groups, such as "Cyber Berkut", have begun to participate in this campaign. Whether or not these groups are independently operating or are under direct command from Russian military or intelligence institutions remains unclear.[4]

Essentially, Russia is using Ukraine as an incubation hub to further enhance its cyber-capabilities by testing and operationalizing various new methods. Starting in 2014, these cyber-attacks moved beyond propaganda into actually harming physical infrastructure, such as destabilizing the Ukrainian power grid and causing blackouts across the country. These cyber-attacks are happening on an industrial scale, sometimes numbering several thousand per month. The attacks are also targeting private-sector companies with malware, which further complicates attempts at cyber-defence, as many computers end up infected with Russian malware without being detected. Unfortunately, most personal and even corporate computers have outdated security systems, making them particularly vulnerable. Overall, these Russian cyber-attacks are more like a bombardment or carpet bombing than a precision strike; they have blanketed Ukraine in an attempt to overwhelm any remaining defences and countermeasures.[5] This ultimately brought the war beyond the front lines, directly into the homes, workplaces and pockets of every Ukrainian citizen.

Unfortunately, Russia's cyber-actions have not stopped at Ukraine's border and they have already led directly to severe consequences for NATO members. The biggest malware attack in history, in both cost and chaos, was NotPetya, a 2017 Russian cyber-operation that was part of their war in Donbas and directly caused crippling financial effects around the world. While Ukraine was NotPetya's intended target, the attack also severely compromised the software of major multinational corporations, such as FedEx, Merck and Maersk, the latter being a Danish shipping giant responsible for around a fifth of the world's shipping capacity.[6] The global financial damage came to a total of around $10 billion. After an investigation, the White House confirmed that the Russian military was behind this attack.[7] Part of the code used in NotPetya was first developed for and tested during major attacks against the Ukrainian power grid in the year prior. The lack of support for Ukraine during this attack directly contributed to the damage NotPetya inflicted on core NATO members like Denmark and France as well as other countries around the world.

[4] Andrew E. Kramer and Andrew Higgins, "In Ukraine, a Malware Expert Could Blow the Whistle on Russian Hacking," *New York Times*, August 16, 2017, https://www.nytimes.com/2017/08/16/world/europe/russia-ukraine-malware-hacking-witness.html.
[5] Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyber War," *Wired*, June 20, 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/.
[6] Ibid., "The White House Blames Russia for NotPetya, the 'Most Costly Cyberattack in History,'" *Wired*, February 15, 2018, https://www.wired.com/story/white-house-russia-notpetya-attribution/.
[7] Ellen Nakashima, "Russian Military was Behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes," *Washington Post*, January 12, 2018, https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html

NATO Cyber-Capabilities

NATO gradually developed and encouraged the growth of Alliance cyber-assets in the years prior to Russia's invasion of Ukraine. This includes the establishment of the Cooperative Cyber Defence Centre of Excellence in Estonia, which facilitates training, exercises and technological research. Further, Alliance professional military educational institutions such as the Germany-based NATO School as well as the NATO Communications and Information Systems School have now integrated cyber-issues into their curriculums.[8] Alliance research hubs such as the NATO Strategic Communications Centre of Excellence have been studying the Russians' operations in Ukraine. Their published reports demonstrate an advanced awareness of Russian cyber-information operations, which they have identified as playing an essential role in the annexation of Crimea and in the ongoing penetrative attacks across the rest of Ukraine. Further, they call for more Alliance resources and attention to be paid to cyber-capabilities.[9]

In September 2014 NATO released an updated formal policy document on cyber-defence, publicly stating it was a core element of modern collective defence. This was an attempt to promote the use of international law on cyber-issues, and to further commit NATO members to investing in cyber-research. This policy document pushed for clearer procedures for Alliance members to request assistance from NATO should they fall victim to a cyber-attack. This document implies that cyber-defence is best handled by a collective defence mindset which links cyber-attacks to Article 5 (the NATO clause that states an attack against one member is an attack against all members).[10]

NATO has taken the first steps to recognizing cyber-space as a new operational domain, similar to air, land and sea. This recognition is the result of an evolving mindset in the Alliance which has shifted from viewing cyber-operations as just a "technical enabler" to being its own area of operations with unique requirements and strategies.[11] Recent public commitments from the Alliance, such as the 2019 London Declaration, also continued to reaffirm with increasing intensity that cyber is an important area for NATO to direct investments.[12] In day-to-day operations, NATO is focused primarily on protecting its digital information and communications networks from malicious malware and foreign hacking.[13] NATO is currently developing a cyber-operations centre to be finalized by 2023, which is intended to streamline and co-ordinate cyber-related operations. Currently, NATO largely delegates cyber-defence to individual Alliance members who are expected to continue to develop their own resources but also contribute to future NATO cyber-needs.[14] Until the centre is ready, NATO is largely relying on the capabilities of the United States and the hierarchy of U.S. military command to co-ordinate cyber-activities

[8] https://ccdcoe.org/.
[9] Robert Szwed, "Framing of the Ukraine-Russia Conflict in Online and Social Media," NATO Strategic Communications Centre of Excellence, May 18, 2016, https://stratcomcoe.org/publications/framing-of-the-ukrainerussia-conflict-in-online-and-social-media/175.
[10] NATO, "NATO Cyber Defence Fact Sheet," July 2019, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf.
[11] Ibid., "Secretary General's Annual Report: 2016," https://www.nato.int/cps/en/natohq/opinions_142149.htm.
[12] Ibid., "London Declaration Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in London, 3-4 December 2019," Press Release, https://www.nato.int/cps/en/natohq/official_texts_171584.htm.
[13] Ibid., Public Diplomacy Division, Press and Media Section, "NATO Cyber Defence," Media Backgrounder, October 2013, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2013_10/20131022_131022-MediaBackgrounder_Cyber_Defence_en.pdf.
[14] Ibid., Cyber Defence Fact Sheet.

and active defence.[15] NATO is currently developing formal doctrine for cyber-operations and has been holding major exercises on the subject; the largest of these exercises was "Cyber Coalition". Held in November 2020, it involved over 1,000 NATO personnel as well as those from partnering groups such as the European Union and even historically neutral states such as Switzerland, Finland and Sweden.[16]

While publicly released information on NATO cyber-operations remains scarce due to its highly classified nature, released documents such as the 2018 NATO Secretary General's Annual Report has stated that the Alliance's offensive cyber-capabilities are lacking, which could pose a problem for developing effective deterrents against aggressive actors.[17] In a May 2018 speech to the Cyber Defense Pledge Conference, NATO Secretary General Jens Stoltenberg highlighted the growing priority NATO gives to cyber-operations. While he acknowledged the NotPetya attack, he did not identify Russian cyber-activities as a main focus for the Alliance. While NATO has clearly been improving its cyber-capabilities in recent years, there unfortunately remains a concern that Russia's disruptive cyber-behaviour may continue to threaten regional actors into the near future.

What's Next?

The potential for future Russian aggression continues to remain a concern for Europe and NATO as the ability for state actors to deny involvement in cyber-attacks means that it will remain an attractive option for coercion. In 2007, Estonia (a NATO member since 2004) fell victim to a destabilizing cyber-attack that lasted several weeks and inflicted considerable damage on the state's digital infrastructure. While the Russian government has never formally claimed responsibility for the Estonia attack, it is highly likely elements of its security services were behind it.[18] The Russian media's coverage of the attacks (which is already scanty), continues to either avoid mentioning their government's involvement in the attacks or implies that Ukraine's infrastructural weakness or the U.S. are to blame.[19] In particular, state-sponsored Russian television stations such as Channel 1 are clearly incentivized to cover up the Kremlin's involvement and push responsibility onto Russia's external adversaries. Attribution thus remains a core problem for cyber-issues.

The use of cyber-attacks in Ukraine has further demonstrated the Russian military's integration of cyber-assets into its operating procedures. A future Russian military intervention will likely look similar. However, to date, NATO aid to Ukraine is not proportional to the situation's severity.

---

[15] Patrick Tucker, "NATO Getting More Aggressive on Offensive Cyber," *Defense One*, May 24, 2019, https://www.defenseone.com/technology/2019/05/nato-getting-more-aggressive-offensive-cyber/157270/.
[16] NATO, "Secretary General's Annual Report: 2020," https://www.nato.int/nato_static_fl2014/assets/pdf/2021/3/pdf/sgar20-en.pdf.
[17] Ibid., "Secretary General's Annual Report 2018," https://www.nato.int/cps/en/natohq/opinions_164187.htm.
[18] Damien McGuinness, "How a Cyber Attack Transformed Estonia," BBC News, April 27, 2017, https://www.bbc.com/news/39655415.
[19] For example, see: "Вирус «Петя» атаковал более двух десятков стран", *Первый Канал,* 28 июня 2017 https://www.1tv.ru/news/2017-06-28/327825-virus_petya; Маргарита Герасюкова, "Вирус нового поколения: как кибератака NotPetya изменила мир," *газета.ru*, 27 июня 2020 https://gazeta-ru.turbopages.org/gazeta.ru/s/tech/2020/06/26/13132537/petya_is_three.shtml.

As the war rages on, NATO's contribution level to Ukraine will likely only strengthen Russia's confidence. Increasing aid and attention to Ukraine during this current crisis will allow NATO to further observe firsthand experiences with cyber-operations and learn the most effective countermeasures against Russian attacks.

All NATO members must continue to treat the cyber-domain extremely seriously and increase its priority in terms of strategic planning. While the Alliance has taken positive steps in developing cyber-resources, more must be done to enhance multilateral co-operation. The threat of cyber-attacks has helped to breathe new life into NATO, and those who care about the Alliance's longevity must continue to push for the integration of cyber-defence into NATO structures. The deterrence NATO offers is one of the best offsets against large-scale destabilizing cyber-attacks, and this can only be effectively undertaken in an Alliance framework. Left alone, individual countries run the risk of falling victim to acts of cyber-aggression. By handling the bulk of cyber-defence through NATO's multilateral structure, member states can diffuse best practices from experiences with ease as well as pool personnel and resources.

Alliance members must continue to increase national investments into developing cyber-resources. There have been tensions in NATO in recent years between the United States and other members over levels of defence spending and overall Alliance commitments. Adding to this tension is the high probability that members' defence spending will also come under pressure as governments direct significant budgetary expenditure to COVID-19-related recovery efforts. Cyber-space and related assets can be a very cost-effective area for countries such as Canada to invest in to demonstrate their Alliance commitments to Washington, without breaking the bank. Effective cyber-operations do not require expensive weapons systems such as warships or fighter jets; they just need well-trained personnel with access to relevant digital networks. Countries such as Canada, which have booming domestic technological sectors, can also turn to public-private partnerships to offset the costs of enhancing cyber-capabilities. By pushing further integration of cyber into a multilateral NATO structure, Canada can play a leadership role in this process, without needing to spend money or even dedicate large numbers of personnel. Cyber-space will be a primary operational domain for NATO in the 21st century, and countries must ensure they are up to the task sooner rather than later.

About the Author

Alexander Salt *is currently a PhD candidate at the University of Calgary's Centre for Military, Security and Strategic Studies. He is a U.S. Marine Corps Gen. Lemuel C. Shepherd, Jr. Memorial Dissertation Fellow and a SSHRC Joseph-Armand Bombardier Doctoral Award holder. He holds an MA in political studies from the University of Manitoba (2014) and a BA (Hons.) in history and political studies from Queen's University (2010).*

Maya Sobchuk *is an undergraduate at Macalester College studying international relations, law and media. She is from Kyiv, Ukraine, the root of her interest in disinformation, cyber-warfare and international relations at large. She has written for the* Kyiv Post *and the U.S. Department of State.*

Canadian Global Affairs Institute

The Canadian Global Affairs Institute focuses on the entire range of Canada's international relations in all its forms including (in partnership with the University of Calgary's School of Public Policy), trade investment and international capacity building. Successor to the Canadian Defence and Foreign Affairs Institute (CDFAI, which was established in 2001), the Institute works to inform Canadians about the importance of having a respected and influential voice in those parts of the globe where Canada has significant interests due to trade and investment, origins of Canada's population, geographic security (and especially security of North America in conjunction with the United States), social development, or the peace and freedom of allied nations. The Institute aims to demonstrate to Canadians the importance of comprehensive foreign, defence and trade policies which both express our values and represent our interests.

The Institute was created to bridge the gap between what Canadians need to know about Canadian international activities and what they do know. Historically Canadians have tended to look abroad out of a search for markets because Canada depends heavily on foreign trade. In the modern post-Cold War world, however, global security and stability have become the bedrocks of global commerce and the free movement of people, goods and ideas across international boundaries. Canada has striven to open the world since the 1930s and was a driving factor behind the adoption of the main structures which underpin globalization such as the International Monetary Fund, the World Bank, the World Trade Organization and emerging free trade networks connecting dozens of international economies. The Canadian Global Affairs Institute recognizes Canada's contribution to a globalized world and aims to inform Canadians about Canada's role in that process and the connection between globalization and security.

In all its activities the Institute is a charitable, non-partisan, non-advocacy organization that provides a platform for a variety of viewpoints. It is supported financially by the contributions of individuals, foundations, and corporations. Conclusions or opinions expressed in Institute publications and programs are those of the author(s) and do not necessarily reflect the views of Institute staff, fellows, directors, advisors or any individuals or organizations that provide financial support to, or collaborate with, the Institute.