5-11-2022

Escalating Russian cyber attacks could risk widening the war in Ukraine

Erika Simpson
University of Western Ontario (Western University), simpson@uwo.ca

THE HILL TIMES
May. 11, 2022
simpson@uwo.ca
escalating-russian-cyber-attacks-could-risk-widening-the-war-in-ukraine

GLOBAL

Escalating Russian cyber attacks could risk widening the war in Ukraine

By ERIKA SIMPSON AND RYAN ATKINSON MAY 11, 2022

To counter Russian escalation, NATO and other European allies must provide extensive support and resources to harden cyber capabilities.

Foreign Affairs Minister Mélanie Joly, left, and Prime Minister Justin Trudeau, centre, in Irpin, Ukraine, with the city's mayor, Oleksandr Markushyn. After the surprise visit, Trudeau announced $50-million in additional military assistance to Ukraine for enhanced intelligence co-operation, cyber security, and cyber operations, write Erika Simpson and Ryan Atkinson. *Photograph courtesy of Twitter/JustinTrudeau*

Cyber attacks by Russia could risk widening the war in Europe as numerous incidents of malware designed to erase hard drives of infected computers, delete data, and wipe programs are being reported. The European Union, United Kingdom, and the United States recently announced Russia was behind a series of cyber attacks in Central Europe on Feb. 24 against a communications company—Viasat—in Ukraine that widely disrupted internet users and wind farms. In April, Russian malware was blocked that would have enabled Russian Military Intelligence (GRU) to create and control botnets,

networks of private computers infected with malicious software. The GRU could have used the botnets for nefarious purposes from illicit surveillance to the deployment of destructive malware.

Russian cyber operations, together with conventional military operations, are detailed in a new April 27 report by Microsoft. The report explained that the Ukrainian government was targeted by 32 per cent of these destructive attacks at the national, regional, and municipal levels. Organizations in the critical infrastructure sector were targeted by 40 per cent of the destructive attacks. Microsoft acknowledged it is unclear whether these tandem effects were due to direct co-ordination or as a result of cyber and military units targeting "a common set of understood priorities." At least six Russian state actors launched more than 237 cyber operations against Ukraine, of which almost 40 destructive attacks were observed by Microsoft, according to a blog post by Tom Burt, a Microsoft corporate vice-president.

Erika Simpson is president of the Canadian Peace Research Association. *Photograph courtesy of Erika Simpson*

Weeks before the war began, on Jan. 13, a suspected GRU-affiliated group, DEV-0586, deployed WhisperGate destructive malware into networks of the Ukrainian government, as well as into organizations in the non-profit and information technology sectors, erasing dozens of systems. One day before the Russian invasion of

Ukraine, the GRU's unit Sandworm deployed FoxBlade wiper malware meant to destroy approximately 300 systems across the Ukrainian government's critical agriculture, energy, finance, information, and technology sectors.

On Feb. 28, threat actors compromised an unnamed media company in Kyiv, and on March 1, the Russian defence ministry warned it would strike military sites in Kyiv "to thwart informational attacks against Russia." Russian missiles struck a Ukrainian television tower, and DesertBlade malware was launched against a major broadcasting company. Together these operations demonstrate escalating levels of cyber attacks on key media outlets that distribute information.

On April 12, Ukrainian authorities thwarted a cyberattack that would have exerted major disruptive consequences on energy capabilities, causing blackouts for an estimated two million Ukrainians. Researchers identified a newer version of Industroyer2 malware similarly used in December 2016 to shut off Ukraine's power. The Sandworm hacker group, confirmed to be Unit 74455 of Russia's GRU military intelligence agency, is being blamed for three cyberattacks targeting Ukraine's energy sector. Sandworm was also behind the NotPetya attack in 2017, which began in Ukraine and spread globally, compromising organizations throughout North America and Europe and causing a total of US$10-billion in damages.

When cyber spillovers occur, cybersecurity leaders from Australia, Canada, New Zealand, the United States, and the United Kingdom (the Five Eyes) have been releasing joint advisories outlining the ongoing risks of malicious cyber activities. The United States' Cybersecurity and Infrastructure Security Agency (CISA) stated that Russia's invasion of Ukraine could expose organizations both within and beyond the region to increased malicious cyber activity as a response to the "unprecedented economic costs imposed on Russia as well as material support provided by the United States and U.S. allies and partners."

Ryan Atkinson is a PhD candidate on cyber defence at Western University and former intern at NATO Headquarters. *Photograph courtesy of Ryan Atkinson*

The North Atlantic Treaty Organization (NATO) allies affirmed in 2014 that cyber defence was part of NATO's core task of collective defence, and, at the the 2014 Wales Summit, announced NATO's response would be determined by the North Atlantic Council on a case-by-case basis. During the 2021 NATO Summit in Brussels, a NATO communiqué emphasized that "significant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack."

The NATO allies will meet in June at the NATO Summit in Madrid to adopt a new strategic concept that promises to "define the security challenges facing the alliance and outline the political and military tasks that NATO will carry out to address them." NATO has already increased its cyber defence support for Ukraine through information sharing, signed agreements of enhanced cyber cooperation, and by granting Ukraine access to NATO's Malware Information Sharing Platform (MISP). NATO has also accorded Ukraine (with other non-NATO member participants including Finland, South Korea, Sweden, and Switzerland) the formal role of "contributing participant" to the NATO Co-operative Cyber Defence Centre of Excellence in Tallinn, Estonia.

Canada is providing enhanced intelligence co-operation, cyber security, and cyber operations to help Ukraine strengthen its ability to defend itself against a range of threats. Additional investments announced by Prime Minister Justin Trudeau in a surprise visit to Kyiv on May 8 include an additional $50-million in military

assistance among other contributions. The next day, during a speech commemorating Russia's Victory Day, President Vladimir Putin called Russia's invasion of Ukraine "inevitable" and the "only correct decision."

To counter Russian escalation, the EU, NATO, NORAD, and Organization for Security and Co-operation in Europe allies must provide extensive support and resources to harden cyber capabilities. But the worst may be yet to come. Russia's invasion was secretly planned in a hierarchical top-down fashion within Putin's inner circle; therefore, malicious protagonists may have needed more time to organize reconnaissance and cyberattacks. The longer the war goes on, without outright conventional victory, the more the cyber war domain could be exploited to attain strategic gains.

Ryan Atkinson is a PhD candidate on cyber defence at Western University and former intern at NATO Headquarters. Erika Simpson is the president of the Canadian Peace Research Association and a professor of international politics at Western University.

The Hill Times