Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR
CYBER SECURITY

CYBER THREAT BULLETIN: Cyber Threat Activity Related to the Russian Invasion of Ukraine

Canada

ABOUT THIS DOCUMENT

AUDIENCE

This Cyber Threat Bulletin is intended for the cyber security community. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/.

CONTACT

For follow up questions or issues please contact the Canadian Centre for Cyber Security at contact@cyber.gc.ca.

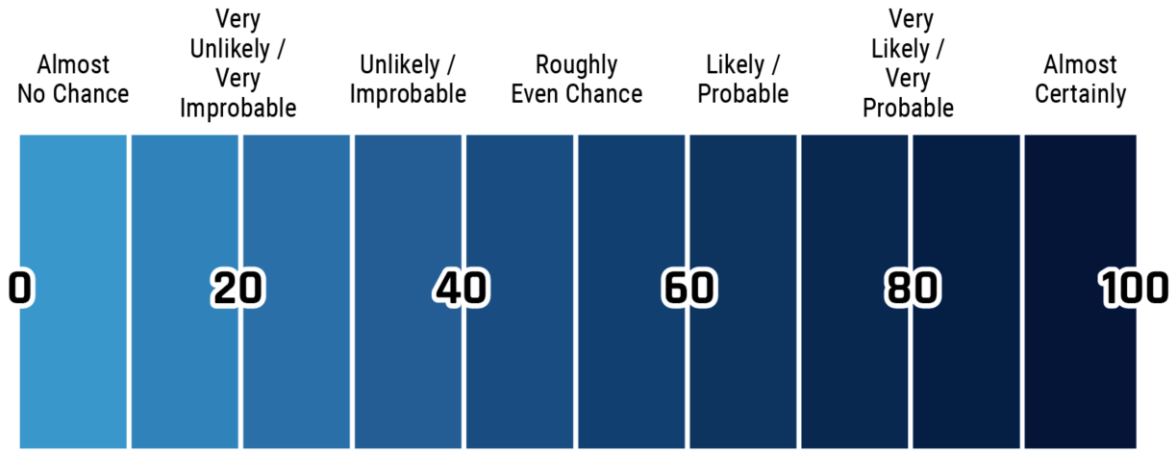
ASSESSMENT BASE AND METHODOLOGY

The key judgements in this assessment rely on reporting from multiples sources, both classified and unclassified. The judgements are based on the knowledge and expertise in cyber security of the Canadian Centre for Cyber Security (the Cyber Centre). Defending the Government of Canada's information systems provides the Cyber Centre with a unique perspective to observe trends in the cyber threat environment, which also informs our assessments. The Communications Security Establishment (CSE)'s foreign intelligence mandate provides us with valuable insight into adversary behavior in cyberspace. While we must always protect classified sources and methods, we provide the reader with as much justification as possible for our judgements.

Our judgements are based on an analytical process that includes evaluating the quality of available information, exploring alternative explanations, mitigating biases and using probabilistic language. We use terms such as "we assess" or "we judge" to convey an analytic assessment. We use qualifiers such as "possibly", "likely", and "very likely" to convey probability.

The contents of this document are based on information available as of 22 June 2022.

The chart below matches estimative language with approximate percentages. These percentages are not derived via statistical analysis, but are based on logic, available information, prior judgements, and methods that increase the accuracy of estimates.



KEY JUDGEMENTS

- We assess that the scope and severity of cyber operations related to the Russian invasion of Ukraine has almost certainly been more sophisticated and widespread than has been reported in open sources.
- We assess that Russian cyber operations have almost certainly sought to degrade, disrupt, destroy, or discredit Ukrainian government, military, and economic functions, secure footholds in critical infrastructure, and to reduce the Ukrainian public's access to information.[1]
- We assess that Russian state-sponsored cyber threat actors will almost certainly continue to perform actions in support of the Russian military's strategic and tactical objectives in Ukraine.
- We assess that Russian state-sponsored cyber threat actors have almost certainly increased cyberespionage targeting of North Atlantic Treaty Organization (NATO) countries in response to NATO's support for Ukraine.
- We assess that Russia is almost certainly in the process of developing cyber capabilities against targets in the European Union (EU) and NATO, including the United States (US) and Canada.[2]

RUSSIAN AND RUSSIA-LINKED CYBER ACTIVITY WITHIN UKRAINE

We assess that Russian cyber operations have almost certainly sought to degrade, disrupt, destroy, or discredit Ukrainian government, military, and economic functions, secure footholds in critical infrastructure, and to reduce the Ukrainian public's access to information.[3] Russian state-sponsored cyber threat actors will almost certainly continue to perform actions in support of the Russian military's strategic and tactical objectives in Ukraine.

Since the 2014 Russian annexation of Crimea, Ukraine has significantly improved its cyber security posture, including with recent assistance from European Union (EU) and Five Eyes (Australia, Canada, New Zealand, United Kingdom, and US or FVEY) governments and technology companies.[4]

Following Russia's invasion of Ukraine on 24 February 2022, likely Russian threat actors conducted several disruptive and destructive computer network attacks against Ukrainian targets, including Distributed Denial of Service (DDoS) attacks and the deployment of wiper malware against various sectors, including government, financial, and energy. Cyber operations have often coincided with conventional military operations (see Figure 1).

To date, there are eight tracked malware families that Russia-linked cyber threat actors have used for destructive activity against Ukraine: WhisperGate/Whisperkill, FoxBlade (HermeticWiper), SonicVote (HermeticRansom), CaddyWiper, DesertBlade, Industroyer2, Lasainraw (IsaacWiper) and FiberLake (DoubleZero).[5]

In mid-April, Russian state-sponsored cyber threat actors launched four different variants of a new malware at various Ukrainian targets. Cyber security firms have attributed these attacks to a group known as Armageddon (aka Gamaredon/Shuckworm), which has been linked to Russia's Federal Security Service (FSB).[6]

Cyber Activity Against Ukrainian Communications

In early March, the Security Service of Ukraine (SBU) reported that cyber threat actors compromised local government and regional authorities' websites to push disinformation about a Ukrainian surrender and a peace treaty signed with Russia.[7]

In early March, the connection to and from SpaceX's Starlink satellite internet terminals, which were providing supplemental internet access to the Ukrainian government, were jammed for several hours at a time, likely by Russian-aligned threat actors. Starlink revised their software and the jamming has not resumed.[8]

In late March, suspected Russia-aligned threat actors caused a major disruption of Ukrtelecom, a Ukrainian internet provider, causing one of the most widespread internet outages in the country since the start of the invasion.[9]

In late April, the Computer Emergency Response Team of Ukraine (CERT-UA) warned of ongoing DDoS attacks targeting pro-Ukraine sites and the government web portal through compromised WordPress sites.[10]

Cyber Activity Against the Ukrainian Energy Sector

In early April, Russian military intelligence (GRU) cyber threat actors Sandworm tried to deploy the Industroyer2 malware and several destructive malware families against high-voltage electrical substations in Ukraine to cause widespread power outages.[11] The Sandworm

actors were able to move from the victim's information technology (IT) network to its industrial control system (ICS) network. CERT-UA, working with Slovak internet security company ESET, were able to remediate and protect the targeted network.[12]

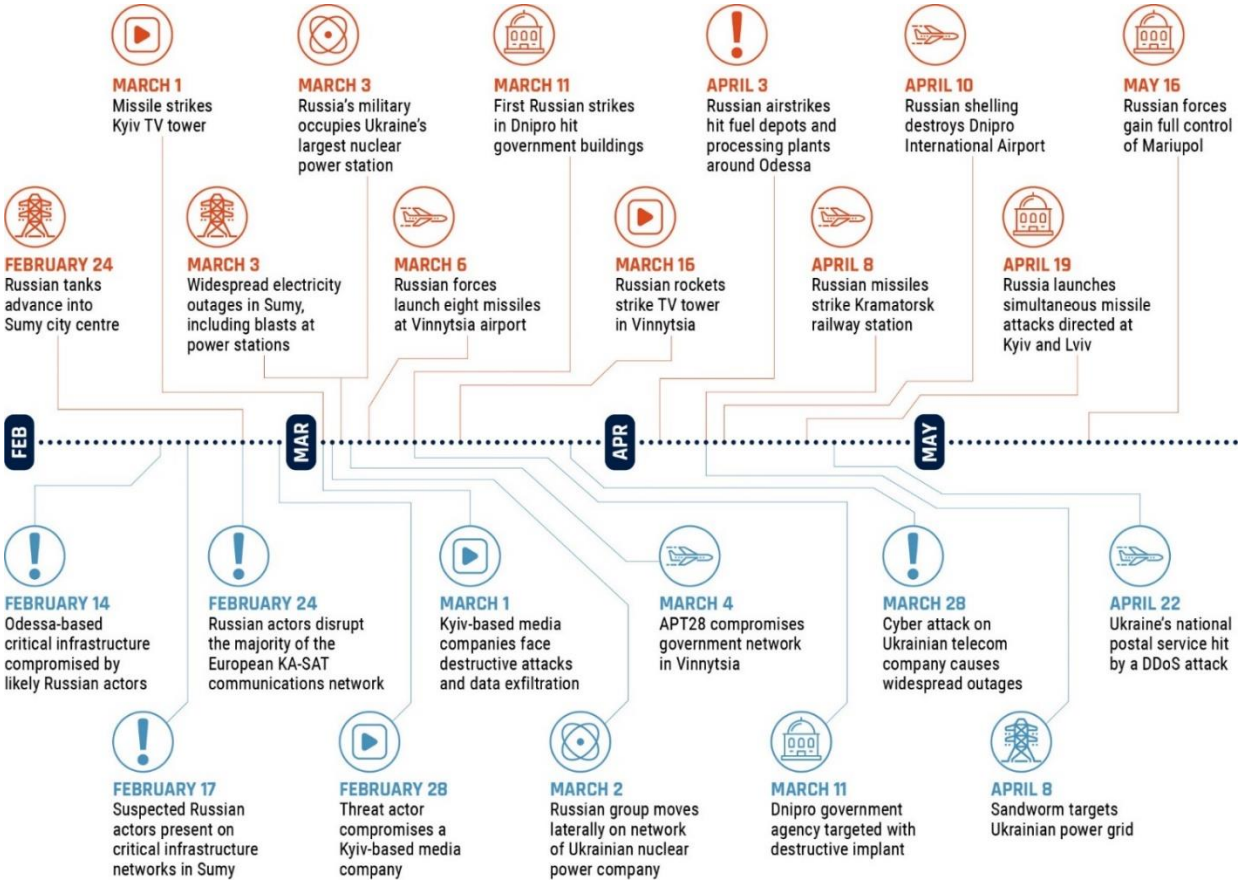
Cyber Activity Against the Ukrainian Government

In May 2022, the Russian hacktivist group XakNet claimed to have breached the Ukrainian Ministry of Foreign Affairs, releasing exfiltrated documents on their social media channel through a hack and leak operation.[13] The XakNet team offered a bounty to their approximately 20,000 subscribers with rewards for the most competent analyses of the data.

Russia-linked cyber actors have repeatedly targeted various Ukrainian government departments with DDoS attacks and various types of wiper malware.[14]

Figure 1: Timeline on Military Attacks and Cyber Operations in Ukraine: 14 February – 16 May[15]

This graph shows examples of significant Russian cyber activity (blue, below the timeline) and kinetic activity (orange, above the timeline).



NOTABLE RUSSIAN AND RUSSIA-LINKED CYBER ACTIVITY BEYOND UKRAINE

While Russian cyber threat activity in relation to the war in Ukraine has been predominantly focused on Ukrainian targets, several incidents have spilled over into other countries, and the threat of spillover effects from Russian cyber operations remains a pressing concern for the international community.

For example, beginning on 24 February 2022, Russian cyber threat actors carried out an operation that disrupted the majority of Viasat's European KA-SAT satellite communications service network, with the intended purpose to disrupt the communications capability of the Ukrainian military.[16] As of 10 March, thousands of KA-SAT satellite network modems were rendered inoperable, including modems located in France, Germany, Greece, Hungary, Italy, and Poland. On 10 May 2022, Canada and FVEY allies, as well as the EU and Ukraine, publicly attributed this attack to the Russian government.[17]

Between 15-22 April, a pro-Russia hacking group, Killnet, claimed responsibility for over 20 DDoS attacks across multiple critical infrastructure sectors in Czechia, Estonia, Latvia, Poland, the UK, and the US.[18]

Targeting the EU and NATO

We assess that Russian state-sponsored cyber threat actors have almost certainly increased cyberespionage targeting of NATO countries in response to NATO's support for Ukraine**.** Since January 2022, Russian cyber actors have targeted government, academic, private sector, and critical infrastructure entities in Denmark, Latvia, Lithuania, Norway, Poland, the US, and Turkey for cyberespionage purposes, as well as entities in Finland and Sweden, both of whom applied for NATO membership following the Russian invasion of Ukraine in February.[19]

In early April, Ukrainian authorities publicly reported several spear-phishing attempts attributed to FSB cyber actors targeting Ukrainian and unspecified EU government targets.[20]

In late April, a previously unknown and financially motivated hacking group (Hive0117) dropped a copy of DarkWatchman malware in a phishing campaign impersonating a Russian agency and targeting Eastern European countries.[21]

In mid-May, an unknown threat actor targeted German users interested in the Ukraine crisis by using a decoy site to lure users into downloading malicious documents, which infected them with a custom PowerShell remote access Trojan (RAT) and stole data.[22]

We assess that Russia is almost certainly in the process of developing cyber capabilities against targets in the EU and NATO, including the US and Canada.[23]

In Canada

From as early as January 2022, evolving intelligence indicates that Russian cyber threat actors are exploring options for potential counterattacks against the United States, Canada, and other NATO/Five Eye allies, including against critical infrastructure.[24] Russian state-sponsored threat actors have already demonstrated the ability to disrupt critical industrial control systems (ICS) through destructive malware. In addition, some pro-Russian cyber actors have threatened to conduct cyber operations against countries/organizations providing material support to Ukraine.[25]

NON-STATE ACTORS TARGETING RUSSIA

In response to a barrage of Russia-linked cyberattacks against Ukraine leading up to and during the invasion, several non-state cyber threat actors came out in support of Ukraine, including by answering the Ukrainian government's call on volunteer hackers to take down Russia's websites.[26]

Hacktivist collective Anonymous–affiliated hacker YourAnonSpider claimed responsibility for the RuTube hack in early May that took down Russia's video platform for at least two days.[27] At around the same time, Anonymous-affiliated group NB65 took credit for breaching the servers of several major Russian television networks and taking them offline.[28]

In March and April, hackers claimed to have breached dozens of Russian businesses and institutions, including one of Russia's primary intelligence services. Anonymous and Network Battalion 65, in collaboration with the transparency collective Distributed Denial of Secrets, claimed responsibility for many of these operations. In mid-June, Anonymous claimed to have hacked Russia's unmanned aerial vehicle (UAV) plans.[29]

KEY PLAYERS ENGAGED IN THIS CYBER ACTIVITY

We assess that the scope and severity of cyber operations related to the Russian invasion of Ukraine has almost certainly been more sophisticated and widespread than has been reported in open sources. Cyber operations have been conducted by threat actors supporting both Russia and Ukraine.

Russian State-Sponsored Cyber Threat Actors

Cyber threat activity against Ukraine has been conducted by various actors linked to the three main Russian intelligence services – the FSB, Foreign Intelligence Service (SVR), and GRU. These cyber actors have been involved in various types of threat activity against Ukraine, including both disruptive and destructive cyber operations.[30]

Pro-Russia Cyber Threat Actors

GHOSTWRITER/UNC1151 is a long-running collection of online foreign influence activities—reportedly associated with the governments of Russia and Belarus. Their activities include disinformation, credential harvesting, hack and leak operations, espionage, and false flag operations.[31]

Cybercriminals & Hacktivists

Supporting Russia:

- Some Russian-speaking cybercrime groups have publicly declared their support for Russia's invasion of Ukraine. For example, the **Conti ransomware group** threatened to retaliate against anyone who conducts computer network attacks on Russian critical infrastructure.[32] Before its recent rebranding and reorganization, Conti was the most impactful ransomware group affecting Canada.
- **Beregini** is a pro-Russia hacker group based in Ukraine consistently targeting the Ukrainian Government and military.[33] Russian hacktivist group **XakNet Team** has also targeted Ukraine.[34]
- **Killnet**, a pro-Russia hacking group, has been conducting a large number of DDoS attacks against websites of countries providing support to Ukraine, especially websites linked to critical infrastructure such as transport. Most recently, on 11 May 2022, Killnet targeted Italy's Defense Ministry, Senate, and National Health Institute.[35]
- **CoomingProject** is another ransomware group that declared its support for the Russian government.[36]

Supporting Ukraine:

- As noted above, members of the hacktivist collective **Anonymous** have launched various cyber operations against the Russian government and Russian industrial firms, including leaking data, wiping files, DDoS operations, and hacking into Russian state television.[37] Another hacking group, the **Belarusian Cyber Partisans**, have also focused on breaching Russian targets, though their impact to date has been limited.[38]
- According to Ukrainian officials, more than 400,000 people have volunteered to help a crowdsourced Ukrainian government effort ("IT army") to protect Ukrainian networks.[39]

KEY INDICATORS ASSOCIATED WITH CYBER SCENARIOS

CSE monitors both classified and unclassified sources of information to determine the strategic intent of cyber threat actors. As Russian cyber activity is rooted in the Russian government's stated policy goals, CSE also monitors classified and open-source reporting on domestic developments in Russia.

While it is difficult to predict future cyber activity, indicators that we are tracking include:

Contextual Indicators:

- An intensification of the conflict in Ukraine, or continued Russian setbacks
- Continued or reinforced NATO support for the conflict
- Continued or intensified economic sanctions or new measures against Russia
- Increasingly aggressive rhetoric from the Russian government
- Declarations of red lines
- Drastic decline in Russian domestic support
- Declarations of specific support to Russia by other state/non-state actors

Cyber Activity Indicators:

- Increased cyber targeting of Canada's allies, particularly the United States
- Increased volume of reconnaissance or scanning activity targeting Canadian/allied government, military, civilian targets
- Increased volume of compromises or attempts to compromise Canadian/allied government, military, civilian targets

- Increased interest in and testing of capability against specific technologies used in critical infrastructure sectors (i.e., ICS devices, uninterruptible power supply (UPS), human-machine interface systems)
- Increased instances of pre-positioning in critical infrastructure networks (i.e., finance, energy, utilities)
- Specific targeting of individuals/entities involved in, or related to, sanctions

MITIGATING RISK, RAISING AWARENESS, AND INCREASING CYBER SECURITY

Since mid-January, the Cyber Centre has reached out to all Canadian critical infrastructure sectors to reinforce the need to enhance vigilance and follow Cyber Centre advice regarding Russian cyber threat tactics, techniques, and procedures. The Cyber Centre has shared information publicly wherever possible, and through trusted channels for more sensitive technical indicators and advice related to the current crisis.

Allied and Cyber Centre Warning Products Released

Beginning in 2021, during Russia's military buildup along the Ukrainian border, and throughout 2022, following Russia's unjustifiable and unprovoked invasion of Ukraine, the Cyber Centre has been monitoring the evolving threat landscape and its impacts—both intentional and spillover—on Canadians and Canadian organizations. Throughout this time period, the Cyber Centre has released eight products to advise, alert, and inform on the threats and possible impacts stemming from the Russian invasion of Ukraine:

Alerts

- AL22-002 – Disruptive activity against Ukrainian organizations - Update 1 (24 February 2022)
- AL22-001 – Wiper malware targeting Ukrainian organizations (17 January 2022)

Joint Cyber Security Advisories

- Joint cyber security advisory on weak security controls and practices routinely exploited for initial access (17 May 2022)
- Joint cyber security advisory on protecting against cyber threats to managed service providers and their customers (11 May 2022)
- Joint cyber security advisory on 2021 top routinely exploited vulnerabilities (27 April 2022)
- Joint cyber security advisory on Russian state-sponsored and criminal cyber threats to critical infrastructure (20 April 2022)

Cyber Threat Bulletins

- Cyber Centre reminds Canadian critical infrastructure operators to raise awareness and take mitigations against known Russian-backed cyber threat activity (13 February)
- Cyber Centre urges Canadian critical infrastructure operators to raise awareness and take mitigations against known Russian-backed cyber threat activity (1 January 2022)

CSE Alerting Canadians on Russian Disinformation Activity

In addition to destructive cyberattacks and cyberespionage efforts, Russian state-sponsored and affiliated cyber threat actors are deploying cyber influence operations that are designed to support its war aims. Starting 1 April 2022, CSE declassified intelligence via its social media account to expose some of the disinformation that Russia is spreading about the conflict in Ukraine:

- On 6 April, CSE flagged that Russia is claiming that the US is establishing military biological labs in former Soviet countries and that Ukraine is being used as a biological testing ground.[40]
- On 13 April 2022, CSE reported that Russia is spreading disinformation about Canadian Forces members committing war crimes in Ukraine and using doctored images to back up false narratives about Canada's involvement in the conflict.[41]
- On 25 April, CSE reported that Russia was deflecting blame for atrocities committed by Russian forces and was making false claims that Ukraine has breached Geneva conventions, causing dissent within the Ukrainian army.[42]

Lack of incident reporting remains a challenge: We strongly encourage Canadian entities in all critical sectors to report compromises or potential compromises to the Cyber Centre. The Cyber Centre relies on this information to generate a more complete picture of cyber threats faced by Canada and refine advice and guidance to guard against evolving tactics.

CSE stands by to help respond to major compromises affecting the Government of Canada (GC) or systems of importance to the GC. In this regard, Cyber Centre may be able to assist with:

- notification, and initial advice and guidance;
- mitigation and containment support;
- log analysis and malware analysis; and
- digital forensics analysis.

Call 1-833-CYBER88 or email contact@cyber.gc.ca to report a compromise or seek guidance.

---

[1] Kapellmann Zafra, Daniel and Raymond Leong, Chris Sistrunk, Ken Proska, Corey Hildebrant, Keith Lunden, Nathan Brubaker. "Industroyer.V2: Old Malware Learns New Tricks." Mandiant. April 25, 2022.
[2] CISA. "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure." April 20, 2022.
[3] Kapellmann Zafra, Daniel and Raymond Leong, Chris Sistrunk, Ken Proska, Corey Hildebrant, Keith Lunden, Nathan Brubaker. "Industroyer.V2: Old Malware Learns New Tricks." Mandiant. April 25, 2022.
[4] Pipikaite, Algirde and Lukas Bester. "How the cyber world can support Ukraine." World Economic Forum. March 19, 2022.
[5] Microsoft. "Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine."
[6] Burt, Jeff. "Russian-linked Shuckworm crew ramps up Ukraine attacks." The Register. April 20, 2022.
[7] Lapienyte, Jurgita. "Ukrainians seize five bot farms used to spread fake news and panic." Cybernews. March 29, 2022.
[8] Duffy, Kate. "A top Pentagon official said SpaceX Starlink rapidly fought off a Russian jamming attack in Ukraine." Business Insider. April 22, 2022.
[9] Coker, James. "Attack on Ukraine Telecoms Provider Caused by Compromised Employee Credentials." Infosecurity. April 6, 2022.
[10] Toulas, Bill. "Ukraine targeted by DDoS attacks from compromised WordPress sites." BleepingComputer. April 28, 2022.
[11] Kapellmann Zafra, Daniel et. al. "Industroyer.V2: Old Malware Learns New Tricks."
[12] Greenberg, Andy. "Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine." Wired. April 12, 2022.
[13] CISA. "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure."
[14] Microsoft. "Special Report: Ukraine."
[15] Figure adapted with content from: Microsoft. Special Report: Ukraine.
[16] Burgess, Matt. "A Mysterious Satellite Hack Has Victims Far Beyond Ukraine." Wired. March 23, 2022.
[17] Global Affairs Canada. "Statement on Russia's Malicious Cyber Activity affecting Europe and Ukraine." May 10, 2022.
[18] Greig, Jonathan. "Italy stops wide-ranging Russian attack of websites of parliament, military, health agency." The Record. May 12, 2022.
[19] Microsoft. "Defending Ukraine: Early Lessons from the Cyber War." June 22, 2022.
[20] CERT-UA. #4378. April 4, 2022.
[21] Toulas, Bill. "Russian govt impersonators target telcos in phishing attacks." Bleepingcomputer. April 27, 2022.
[22] MalwareBytes. "Custom PowerShell RAT targets Germans seeking information about the Ukraine crisis." May 16, 2022.
[23] CISA. "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure." April 20, 2022.
[24] CISA. "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure."
[25] CISA. "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure."
[26] Shore, Jennifer. "Don't Underestimate Ukraine's Volunteer Hackers." Foreign Policy. April 11, 2022.
[27] Collier, Kevin. "A Cyberattack Took Down One of Russia's Largest Video Platforms for Days." NBC News. May 11, 2022.
[28] Hackread. "Anonymous Affiliate NB65 Breach State-Run Russian Broadcaster; Leak 786B of Data." April 6, 2022.
[29] YourAnonSpider. "Russian UAV drones plans and tactics hacked." June 10, 2022.
[30] Microsoft. "Special Report: Ukraine."
[31] Roncone, Gabriella and Alden Wahlstrom, Alice Revelli, David Mainor, Sam Riddell, Ben Read. "UNC1151 Assessed with High Confidence to have Links to Belarus, Ghostwriter Campaign Aligned with Belarusian Government Interests." Mandiant. November 16, 2021.
[32] Reichert, Corinne. "Conti Ransomware Group Warns Retaliation if West Launches Cyberattack on Russia." CNET. February 25, 2022.
[33] Wahlstom, Alden and Alice Revelli, Sam Riddell, David Mainor, Ryan Serabian. "The IO Offensive: Information Operations Surrounding the Russian Invasion of Ukraine." Mandiant. 19 May 2022.
[34] CISA. "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure."
[35] Petkauskas, Vilius. "Hacker wars heat up as the pro-Russian Killnet attacks Italy." Cybernews. May 23, 2022.
[36] CISA. "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure."

[37] David, Benjamin. "Russian Ministry Website Reportedly Hacked." InfoSecurity. June 6, 2022.
[38] Roth, Andrew. "'Cyberpartisans' hack Belarusian railway to disrupt Russian buildup." The Guardian. January 25, 2022.
[39] Stokel-Walker, Chris and Dan Milmo. "'It's the right thing to do': the 300,000 volunteer hackers coming together to fight Russia." The Guardian. 15 March 2022. Shore, Jennifer. "Don't underestimate Ukraine's volunteer hackers." Foreign Policy. 11 April 2022.
[40] CSE Official Twitter Account @cse_cst. 6 April 2022.
[41] CSE Official Twitter Account @cse_cst. 13 April 2022.
[42] CSE Official Twitter Account @cse_cst. 25 April 2022.

CAT. D96-88/2022E-PDF
ISBN 978-0-660-44578-6