MARCH 2022

RETURNING TO THE WILDERNESS OF MIRRORS

How Great Power Competition and Cyberwarfare Could Precipitate a Digital-Age Cold War

Part of the ICIT Weapons of Mass Disruption Series

Authored By:
Drew Spaniel, Lead Researcher, ICIT

Contributors Include:
Michael Aisenberg, ICIT Fellow & Principal Cyber Policy Counsel, MITRE Center for National Security
Tim Callahan, ICIT Fellow & SVP & Global CISO, Aflac
Parham Eftekhari, Founder & Chairman, ICIT & EVP, CISO Community, Cyber Risk Alliance
Donald Heckman, ICIT Fellow & Defense Cyber Solutions Leader & Director,
Joyce Hunter, Executive Director, ICIT
Itzik Kotler, ICIT Fellow & Co-Founder & CTO, SafeBreach
Don Maclean, ICIT Fellow & Chief Cybersecurity Technologist, DLT
Stan Mierzwa, ICIT Fellow & Director, Center for Cybersecurity, Kean University
Jim Routh, ICIT Fellow & Advisor, Board Member, & Former CSO
Pete Slade, ICIT Fellow & CTO, ThreatWarrior

ICIT Institute for Critical Infrastructure Technology
The Cybersecurity Think Tank

Returning to the Wilderness of Mirrors

How Great Power Competition and Cyberwarfare Could Precipitate a Digital-Age Cold War

March 2022

ICIT would like to thank the following experts for their contributions to this paper:

- Michael Aisenberg, ICIT Fellow & Principal Cyber Policy Counsel, MITRE Center for National Security
- Tim Callahan, ICIT Fellow & SVP & Global CISO, Aflac
- Parham Eftekhari, Founder & Chairman, ICIT & EVP, CISO Community, Cyber Risk Alliance
- Donald Heckman, ICIT Fellow & Defense Cyber Solutions Leader & Director, Cybersecurity Solutions, Guidehouse
- Joyce Hunter, Executive Director, ICIT & Former Interim CIO and Deputy CIO, USDA
- Itzik Kotler, ICIT Fellow & Co-Founder, and CTO, SafeBreach
- Don Maclean, ICIT Fellow & Chief Cyber Security Strategist, DLT
- Stan Mierzwa, ICIT Fellow & Director and Adjunct Professor, Center for Cybersecurity, Kean University & CTO, Vennue Foundation
- Jim Routh, ICIT Fellow and Chief Security Advisor, Virsec
- Pete Slade, ICIT Fellow & CTO, ThreatWarrior

Contents

Abstract

The purpose of this publication is not to comprehensively recount current events, rehash media reports, or presume the current state of the Russian-Ukrainian conflict. Instead, this publication aims to objectively set a macro-level understanding of socioeconomic and geopolitical impacts on Russia, provide a baseline of the tools, tactics, procedures, methodologies, and strategies attributed to Russia, and establish a cybersecurity lens through which readers can better interpret the developing events and more effectively adapt to secure public and private U.S. critical infrastructure against potential retaliatory offensive campaigns.

Microscopic analysis of the conflict is likely premature and would rely at least as much on supposition as fact. Further, an exhaustive, in-depth analysis may be overwhelmingly for a broad audience. Due to the evolution and responses to the conflict at the time of this writing, ICIT, in partnership with our esteemed fellows, anticipate that this publication will be the first in a series documenting the nation-state weaponization of disruptionware in response to geopolitical or socioeconomic impetuses.

Introduction

At the height of the Cold War, Former CIA Chief of Counterintelligence James Jesus Angleton often borrowed from T.S. Eliot's poem, "Gerontion," to describe Soviet operations as a "Wilderness of Mirrors." According to a three-page memo included in documents that his family donated to Georgetown University Library after his death, he meant, "[A] myriad of stratagems, deceptions, artifices, and all the other devices of disinformation which the Soviet bloc and its coordinated intelligence services use to confuse and split the West … an ever-fluid landscape where fact and illusion merge." Historical accounts of Angleton aside, the application of Eliot's metaphor to Russian operations holds as true today as it did during the Cold War, and as we will detail later, many of the modern strategies and tactics directly evolved from Cold War doctrine.

Over the past two decades, at least twenty-five distinct, high-profile nation-state-sponsored advanced persistent threat (APT) groups that excel at cyberespionage and disruptive attacks have been attributed to Russia. Further, Russia has an international reputation for granting safe haven to cybercriminals and later deputizing or empowering to launch attacks against foreign infrastructure. Sophisticated malware is frequently disseminated from APT groups to lower sophistication attackers to obfuscate attack campaigns or commissioned from cyber-mercenaries for APT adaptation and use. Investigations into the tools, techniques, and infrastructure of Russian threat actors have indicated that they occasionally launch digital false flag operations by masquerading as another digital group and intentionally planting forensic markers so that the attack may precipitate into an international conflict or domestic discord. It should be noted that false flag attacks originating from Russia and masquerading as Russian actors may be one of the understated and under-measured outcomes of the developing fallout of the Russia-Ukraine conflict. Finally, Russia may be one of the reasons that some are questioning whether we have moved from the digital age into the age of disinformation. The "Internet Research Agency" tactically succeeds the preceding KGB and GRU efforts to sow disinformation and discord abroad by leveraging cadres of low-sophistication online trolls to redirect narratives, disrupt movements, and otherwise destabilize its geopolitical rivals via large- and small-scale influence operations.

An exhaustive detailing of Russian cyber operations could fill books and is better suited for the analyses within technical whitepapers. As the specific APT groups and their preferred malware vary over time, the focus of this initial publication will instead center on establishing a baseline understanding of Russian cyber strategy and evolving operations.

A Brief Macroscopic Primer on Recent Socioeconomic Impacts on Russia

On February 24, 2022, Russia launched a large-scale invasion of Ukraine, an escalation of their ongoing 2014 conflict. Subsequently, the global community condemned Russia for escalating the conflict, and at the time of this writing, the United States, United Kingdom, European Union, Canada, Japan, Australia, New Zealand, Switzerland, South Korea, Singapore, and Taiwan have expanded or imposed sanctions or economic disincentives against Russia [1]. Further, many private companies, social media platforms, and global cooperatives, such as the SWIFT banking system, are no longer permitting operations within Russia until a cessation of aggression and a withdrawal of forces can be demonstrated. Even the Bank of China and Industrial and Commercial Bank of China (ICBC) placed limited financing to purchase Russian raw materials [2] [3]. Russian billionaires lost an estimated $40 billion on the day of the invasion, and in the week since, the ruble slid as much as 30% against the dollar, and the Russian economy fell 39%, according to the RTS Index [4] [5]. Two days later, the S&P Global Rating downgraded the Russian government credit rating to "junk," which may force funds that require investment-grade bonds to dump Russian debt [5]. On February 27, 2022, BP, one of the world's seven largest oil and gas companies and the single largest foreign investor in Russia, announced it was divesting from Rosneft, which could cost the company as much as $25 billion. The Rosneft interest comprises about half of BP's oil and gas reserves and a third of its production [5]. Others such as the Government Pension Fund of Norway, Shell, ENI, Maersk, and Mediterranean Shipping also divested or suspended operations [5]. Former Russian Deputy Finance Minister Sergei Aleksashenko described the initial and immediate impact as, "This is a kind of financial nuclear bomb that is falling on Russia." Worse, the global response to the conflict and the socioeconomic pressures being imposed on the people of Russia have led to unprecedented protests against the Kremlin, the rebuke of over one hundred and fifty senior officials in a written statement, and discontent of many of the oligarchs within Putin's inner circle [6] [7]. Don Heckman, ICIT Fellow and Defense Cyber Solutions Leader & Director, Cybersecurity Solutions, Guidehouse, cautions, "As the United States, European nations and a majority of the countries of the world impose sanctions against Russia to affect its economy to impact its ability to sustain its military offensive, it is likely that Russia will launch retaliatory offensive cyber campaigns targeting the United States and its allies critical infrastructure to try and inflict damage to our economies."

In a sense, the impact of the sanctions is divorced from the likelihood of retaliatory attack campaigns in that as a matter of pride and an exertion of force in the Great Power competition, Russia is likely to attempt cyberattacks against every nation that condemned its actions, imposed sanctions, or otherwise acted to restrict its international leverage or exert pressure on Russia during the conflict. Some analysts speculate that Russian President Vladimir Putin anticipated the imposition of sanctions, and he may have begun intentionally transitioning Russian infrastructure to be more resistant to potential sanctions since the start of the conflict with Ukraine in 2014. As a result, he responded to the recent socioeconomic and geopolitical pressures by capitulating between making broad dismissals of the impact of sanctions and delivering bombastic threats, such as in his February 24, 2022 address, stating, "Whoever tries to hinder us" will face "consequences that you have never faced in your history." Russian APTs have an established history of targeting immediate or delayed cyberespionage and disruptionware attacks on the critical infrastructure of their geopolitical rivals. Parham Eftekhari, ICIT Founder and Chairman and EVP, CISO Community, Cyber Risk Alliance, posits, "If Russia chose to retaliate against sanctions and other US support for Ukraine, targeting energy, financial, and communication sectors would inflict maximum damage to the economy and have ripple effects to other sectors." He adds, "Owner-operators in these sectors should be particularly vigilant, particularly if the conflict continues and Putin's ire towards the US grows." Michael Aisenberg, ICIT Fellow and Principal Cyber Policy Counsel, MITRE Center for National Security, also warns that a whole-of-nation effort to improve cybersecurity is needed to preempt potential attacks from Russia or other opportunistic adversaries. He warns, "US Control, Communications, and. Intelligence infrastructure would be high-value targets but so would support infrastructures that are often under-considered and under-secured against APT threats, such as financial networks, water systems, air traffic control networks, automated transit systems, Internet infrastructure, and other systems at the state, local, or private sector level."

Feigning reassurance in a March 1, 2022, conference call with reporters, Kremlin spokesperson Dmitry Peskov said, "Judging by the measures that many countries are taking against us, they are now all de facto unfriendly… response to these unfriendly, hostile actions, must be analyzed, no one is going to shoot ourselves in the foot to harm someone. We do what we need to, what suits us, and we're doing it with a sober head." Many on the global stage interpreted President Putin's statement as an implicit threat of digital retaliation for the socioeconomic impacts he perceives as injustices against his country. Yet, Peskov's comment may be more revealing in anticipation of strategy. While Russia may do some public displays of cyber or cyber-kinetic force, as they did with the December 2015 Black Energy cyberattack on the Ukrainian power grid, in keeping with past APT attacks, their APT groups are likely to be more judicious, patient, and subtle in their upcoming offensive campaigns.

Cold Warfare Evolved

Russia, arguably more than any other nation-state actor, seems to have devised a way to integrate cyber operations into a strategy capable of achieving political objectives. Russia's approach in its past power struggles with NATO and the West indicates that it does not intend to attempt to match the physical military power of its rivals in the Great Power competition. Instead, as in the Cold War, it relies on eliciting strategic advantages without outright provoking an armed response. This core element of Russian security policy is exemplified by the Gerasimov doctrine (Russian non-linear war), which posits that "[t]he role of non-military means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of weapons in their effectiveness." In short, Russia’s Information Warfare is broadly cyberespionage and prepositioning during peacetime and disruptive and destructive attacks during conflict. This evolution of Cold War tactics has been referred to as a Digital Maskirovka [9].

Inside the Digital Maskirovka

While all militaries seek to misdirect enemies, Russia's military doctrine of deception – known as maskirovka, Russian for "masking" or "camouflage" – is a foundational component of the Russian military and intelligence. With maskirovka, the fog of war is not merely the natural byproduct of combat but a deliberately manufactured feature of military operations intended to increase ambiguity and indecision in opposing forces. Using decoys, clandestine actions, and disinformation, maskirovka facilitates military resilience and surprise action and increases doubt in an adversary while obfuscating Russian weaknesses [9].

The tools of maskirovka broadly include psychological operations, manipulation of media, disinformation and propaganda, electronic and cyber warfare, unidentified irregular forces and unattributed mercenaries, and proxies and physical deception through camouflaged military maneuvers. Maskirovka, in its modern iteration, takes place at the boundary of conventional conflict – the gray zone between peace and war. Some recent old-school applications of the tactics in physical conflicts included: the decoys tanks used by the Serbian military during the NATO air campaign in Kosovo in 1999; confusing demonstrations of capability, such as the Zapad wargame; occasional "buzzing" of US naval vessels or near contested borders to determine response protocols; deployment of "patriotic" or "volunteer" unconventional forces, such as the "little green men" deployed to annex Crimea in 2014; the clandestine delivery of military supplies camouflaged as humanitarian convoys to support proxy and clandestine forces; incessant denial of military presence or disingenuous narratives behind military operations, etc. [9].

Maskirovka is a holistic strategy, and it often combines physical, cyber, and disinformation elements. A 2017 report by the Center for Naval Analysis (CAN) explained, "The Russians generally do not use the terms cyber (kiber) or cyber warfare (kibervoyna), except when referring to Western or other foreign writings on the topic. Instead, like the Chinese, they tend to use the word informatization, thereby conceptualizing cyber operations within the broader rubric of information warfare (informatsionnaya voyna)." For instance, a disinformation campaign ran parallel to the troop buildup near South Ossetia ahead of the 2008 invasion of Georgia (and repeated before the 2014 annexation of Crimea), which allegedly involved Russian special operations forces with no insignia clearly identifying them as Russian military, later dubbed "little green men" [9].

Offensive cyber and electronic warfare capabilities allow Russia to insert doubt into their enemy's faith in digital systems. Fake command and control facilities emit fake radio frequency signals to deceive enemy intelligence assets while manipulating or jamming radio frequency or GPS signals could undermine a military commander's faith in the accuracy of precision-guided munitions. With modern communications technology, automated bots and human actors on social media platforms amplify targeted disinformation to both divide populations and entice susceptible groups to favor Russian-produced narratives. State-sponsored media – such as RT and Sputnik – can guide the conversation and help legitimize Kremlin propaganda. Open-source platforms can be used to discredit the Kremlin's disinformation, potentially causing unforeseen political backlash. However, successfully countering the narrative requires a swift and agile reaction [9].

Maskirovka creates enough uncertainty and plausible deniability to delay timely or meaningful responses. In the past, this helped the Kremlin sidestep international norms without evoking significant global repercussions. For instance, Russian "patriotic hackers" likely executed the electronic denial of service attacks against Estonia – a NATO member – in 2007, but Russia maintained plausible deniability, complicating Estonia and its allies' ability to retaliate without escalating to a physical conflict. Maskirovka often goes beyond fostering doubt and presents an alternative – and often false – narrative. Russia has used this to pursue geostrategic objectives under the guise of international cooperation. Perhaps the most prominent example is Russia's positioning itself as a counterterrorism partner in Syria – and Libya to a lesser extent – as it sought to extend its global influence in the Middle East. Russia also acted as a strategic ally to the international community in the war against ISIS, a potential foundation for the alleviation of the sanctions initially imposed on Moscow for its annexation of Crimea [9].

Known Russian Agencies and Reported Activities

Russia maintains numerous units that are overseen by various security and intelligence agencies such as the Main Directorate of the General Staff (GRU), the Foreign Intelligence Service (SVR), the Federal Security Service (FSB), the Federal Protective Service (FSO), and the Internet Research Agency [8].

Table 1: Description of Russian Agency Cyber Roles and Responsibilities

Entity	Function	Operations
Main Directorate of the General Staff (GRU)	Primary Military Intelligence Agency	APT groups, malware research and development institutes, Unit 54777 (disinformation and online influence operations).
Foreign Intelligence Service (SVR)	Primary Civilian Foreign Intelligence Service	The collection of foreign intelligence using human, signal, electronic, and cyber persistence.
Federal Security Service (FSB)	Primary Domestic Security Agency	Internal security, counterintelligence, defensive cyber operations, and monitoring domestic criminal hackers (jointly undertaken with Department K of the Ministry of Internal Affairs), training and research centers, and some foreign intelligence collection and offensive cyber campaigns (usually false flag attacks, adapted/mimicked malware, or obfuscated tactics). The 16th Center houses most of the FSB's signals intelligence capabilities, and the 18th Center for Information Security directs domestic operations and security and conducts some foreign operations such as focused targeting of energy sector and other critical infrastructures.
Federal Protective Service (FSO)	Responsible for the Physical and Electronic Security of the Government and Government Personnel	Extensive signals and electronic operations and communications security The FSO appears primarily concerned with the defense of Russian government networks, and there is no indication it has launched offensive operations.
Internet Research Agency	A Private Organization Funded by Kremlin-connected oligarch Yevgeniy Prighozin	Disinformation and propaganda operations in support of the Russian government and agency influence and disruption operations.

Prolific Russian APT Groups

A catalog of the few dozen APT groups attributed to the Russian state since 2000 is outside the scope of this publication, but future entries in ICIT's Weapons of Mass Disruptionware series will likely include in-depth technical and non-technical information about the prolific Russian APTs in the context of their attacks or potential impacts on US critical infrastructure. As a high-level summary, Russian APTs tend to focus on either cyberespionage or disruptionware. Don Heckman provides, "We have seen Financial, Communications, and Energy sectors frequently targeted by disruptionware in prior Russian state-sponsored attacks. In 2007, a denial-of-service attack was used to disrupt the financial markets and government operations in Estonia over disagreements with Russia. Russia also initiated cyberattacks against financial institutions in both Georgia and Crimea prior to and during the invasions. Another attack concentrated on the Ukraine Power Grid, resulting in power outages for over 230,000 users. This attack, the first publicly acknowledged successful cyberattack on a power grid, remotely shut off substations, and disabled or destroyed IT infrastructure components."

While some threat actors disband when their operations are uncovered, a few Russian APTs have remained active and evolved for about the last decade. Some of the top threat actors are featured in the following table based on industry whitepapers and the MITRE ATT&CK resource. For the sake of building a better collective understanding across stakeholders in the cybersecurity community, ICIT is providing the common name associated with the campaign as well as what we believe may be associated names based on indicators of compromise, tools, tactics, and procedure profiles, and publicly available whitepapers. The names derive from different vendors and research organizations monitoring the threats according to their own frameworks. As a judicious mention, attribution is not an exact science, especially with the potential for false flag operations, cyber-mercenaries, obfuscation tactics, and different vendor research paradigms. Nevertheless, the value in detailing commonalities informed from academic research, technical whitepapers, and industry blogs serve to provide a simulacrum through which a broader audience can approximate the threat and develop a better understanding of adversarial efforts. More simply, attribution and APT profiles provide a non-technical audience with an antagonist to process narratives and build a foundation of understanding around.

Table 2: Prolific Russian Advanced Persistent Threat Groups

Attribution	Associated Names	Example Past Targets
Sandworm State-Sponsored GRU GTsST military unit 74455	BlackEnergy, Quedagh, Voodoo Bear, MITRE G0034, ELECTRUM, Telebots, IRON VIKING	Destructive disruptionware against Energy infrastructure, wiper malware against Energy and Government targets, and denial of service and botnet malware against IoT and IIoT devices.
Energetic Bear State-Sponsored FSB	Crouching Yeti, Dragonfly 1.0, Koala Team, MITRE G0035, TG-4192	Cyberespionage against Energy, Education, Information Technology, Healthcare, Construction, and Government entities. Disruptionware against Energy, ICS, communications, and Government systems.
Dragonfly 2.0 State-Sponsored FSB	IRON LIBERTY, DYMALLOY, Berserk Bear, MITRE G0074	Cyberespionage against US government entities and Energy, Nuclear, Commercial Facilities, Water, Aviation, and Critical Manufacturing sectors
APT28 State-Sponsored GRU GTsSS military unit 26165	Sofacy, Sednit, Fancy Bear, Grizzly Steppe (with APT 29), Pawn Storm, MITRE G0007, SNAKEMACKEREL, Swallowtail, Group 74, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127	Cyberespionage against US Government agencies and election infrastructure. Disruptive influence operations occasionally run in parallel.
APT29 State-Sponsored SVR	Cozy Duke (and the Duke family broadly), Cozy Bear, HammerToss, Grizzly Steppe (with APT28), MITRE G0016, NobleBaron, Dark Halo, StellarParticle, NOBELIUM, UNC2452, YTTRIUM	Cyberespionage against US and NATO Government agencies, research, and think tanks. Attacks on Election infrastructure in US, EU, Central Asia, East Africa, and Middle East. Supply-chain attacks against the US and EU (SolarWinds). May also contribute to false flag campaigns and influence operations.
Turla Group **State-Sponsored**	Uroburos, Venemous Bear, Snake, Krypton	Cyberespionage against the government, embassies, military, education, research, and pharmaceutical companies
Carbonak **Cyber Criminal Collective**	Anunak	Fiscally motivated attacks against Financial systems across the EU
Fin7 **Cyber Criminal Collective**	GOLD NIAGARA, ITG14, Carbon Spider, MITRE G0046	US retail, restaurant, and hospitality sectors. Targeted ransomware against "high-value" targets since 2020.

Additional information, including indicators of compromise (IoCs), attributed malware, and whitepaper sourcing for each attributed name, can be found within the MITRE ATT&CK Resource.

Past Examples of Russian APT Activity

Within cyberspace, Russia relies on the weaponization of cybercriminals to disrupt foreign economies and infrastructure belonging to private sector rivals. Meanwhile, its APTs focus on the development and deployment of sophisticated, persistent malware capable of cyberespionage, disruptive/destructive impacts, or both. As previously mentioned, in December 2015, the Russian state-sponsored Sandworm APT publicly deployed the BlackEnergy malware against the Ukrainian power grid, likely as a global show of force and demonstration of capability. Reportedly, the United States later found the BlackEnergy malware prepositioned on systems belonging to multiple federal agencies; however, in those cases, it is believed that the malware was deployed for its cyber-espionage capabilities. Sandworm is believed to have launched the June 2017 NotPetya attacks that primarily targeted Ukraine. ICIT characterizes both the BlackEnergy and NotPetya campaigns disruptionware attacks. In the case of the former, the functional goal of the deployed malware was to render the Ukrainian power grid inoperable. In the later attack, the Petya ransomware was specifically modified so that it self-propagated and systems it encrypted could not be reverted. Due to its self-propagation, NotPetya affected computer networks worldwide, targeting hospitals and medical facilities in the United States and costing more than $1 billion USD in downtime and damages. Neither attack against Ukrainian infrastructure was financially motivated or appeared focused on data exfiltration. The goal was disruption.

Another notable example of the multi-vector, hybrid Maskirovka strategy was revealed in the DHS investigation into Russian APT28 and APT29's (collectively referred to as Grizzly Steppe in this case) concerted attempts to influence the 2016 US Presidential election by attempting to digitally compromise critical election systems while simultaneously propagating disinformation campaigns across social media. It is unlikely that Russian actors were confident in their ability to technologically alter the result of the election; even with the cybersecurity and cyber-hygiene problems present in the 2016 election systems and processes, too many systemic counterbalances would have called a false result into question. Instead, the goal of the reported influence operations and attempted digital compromises may have been to sow discord and division within the US population and plant the seed of distrust in the election process in the minds of some US communities [14] [15].

APT Activity in Response to the 2022 Invasion of Ukraine

Since the resurgence of the conflict in Ukraine, Russian threat actors have not been idle. In late February 2022, over 70 Ukrainian government websites and banking infrastructure were subject to disruptive attacks. A few days later, the United Kingdom's National Cyber Security Centre, CISA, the NSA, and FBI released a joint Cybersecurity Advisory (CSA) reporting the Sandworm APT were deploying a new malware, referred to as Cyclops Blink. CISA and the NCSC describe the Cyclops Blink malware as a successor to an earlier Sandworm tool known as VPNFilter, which infected half a million routers to form a global botnet before it was identified by Cisco and the FBI in 2018 and largely dismantled. VPNFilter was deployed in stages, with most functionality in the third-stage modules. These modules enabled traffic manipulation destruction of the infected host device and likely enabled downstream devices to be exploited [10].

The FBI, CISA, and NSA also published a joint CSA regarding Russian state-sponsored cyber actors' ongoing efforts over the last several years to target US cleared defense contractors. The advisory, entitled "Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain

Sensitive US Defense Information and Technology," details the industries and information Russian actors have targeted, common adversary tactics, detection, and incident response actions, and mitigation recommendations. NSA and its partners assess that continued targeting is likely and recommend organizations apply the mitigations shared in the joint Cybersecurity Advisory. They also encourage all US cleared defense contractors (CDC) — with or without evidence of compromise — to apply the mitigations in the advisory to reduce the risk of compromise by Russian state-sponsored cyber actors. While these mitigations are not intended to be all-encompassing, they address common TTPs observed in these intrusions and will help to mitigate against common malicious activity [11].

Finally, CISA and the FBI also released a joint advisory to warn organizations about the HermeticWiper and WhisperGate malware, two destructive malware variants that have been used to target organizations in Ukraine and render compromised systems inoperable. Threat actors deployed the HermeticWiper malware against systems in Latvia, Lithuania, and Ukraine hours before Russia's invasion of Ukraine [12]. Although there have been no reports of HermeticWiper being used against US organizations, HHS' Health Sector Cybersecurity Coordination Center (HC3) assessed the destructive nature of the malware and threat to US healthcare systems significant enough to merit to issue its own warning and recommendations to domestic healthcare networks [13].

It should not be understated that retaliatory cyberattacks may not be immediate or may come in waves. The Maskirovka strategy excels at destabilizing adversaries and sometimes draining their resources by holding them in anticipation until their vigilance erodes. Some Russian APTs focus on immediate disruptive or destructive impacts, while others are famous for their persistence and ability to laterally propagate onto other networks. Itzik Kotler, ICIT Fellow and Co-Founder, and CTO, SafeBreach, advises, "While there are cyber campaigns targeted at US critical infrastructure providers from time to time, the biggest risk at this moment likely exists for any US-based companies that have subsidiaries in Ukraine, are leveraging contractors in Ukraine for outsourcing or offshore development or are working with third parties that have Ukrainian subsidiaries or contractors. Because of the digital and interconnected nature of our work environments, US offices are likely connected to their Ukrainian counterparts in these instances via VPNs or other communication infrastructure. If Ukrainian locations experience a malware attack, it is only a matter of time before the attack accesses a computer with a VPN link to US-based networks, computers, and facilities."

A Warning: International Turmoil Increases Offensive Opportunities for All Adversaries

Stan Mierzwa, ICIT Fellow and Director and Adjunct Professor, Center for Cybersecurity, Kean University & CTO, Vennue Foundation, relates, "Staying situationally aware to large scale events and how cybersecurity threats emerge is an important element for any organization to put up their best cyber defense. With the current events developing in Eastern Europe and the resulting global impacts, a parallel can be drawn to the recent COVID-19 pandemic. The pandemic was a public health issue, and yet, there was an increase in cybercriminal behavior and cyberespionage activities because the resources and attention were diverted elsewhere." In fact, a few international examples have metastasized immediately after the invasion. In late February 2022, CISA released an advisory warning of increased activity from the Iranian MuddyWater APT, and China pressured the Taiwanese border [16] [17].

The exertions and turmoil of international conflicts can stress the resources, attention, and defenses of entire nations. In the case of the specific countries physically engaged in the conflict, there may not even be personnel on-site to secure systems or respond to incidents. Parham Eftekhari explains, "Global conflicts between nation-states can be exploited by opportunistic adversaries who can obfuscate their attacks. The current threat facing US critical infrastructure is not solely from Russia, but other state-sponsored and criminal APTs who will use this opportunity to attack for ideological, geopolitical, or financial motivations." In addition to potential retaliatory cyberattacks, critical infrastructure organizations must also be on guard against the activities of other adversaries. Some potential scenarios include:

- False flag cyberattacks originating from any side of the conflicting nations or from emboldened lower-sophistication hactivist or "patriotic" attackers
- Disruptive cyberattack campaigns from domestic script kiddies and cybercriminals
- Opportunistic cybercriminals exfiltrating data or deploying ransomware
- Scam campaigns capitalizing on the conflict (donation scams, phishing, ransomware, etc.)
- DDoS attacks against coordination and public-facing resources, online defacement, social media hijacking, etc.
- Opportunistic nation-state sponsored attacks

Michael Aisenberg further warns that as the US has seen with some prior national emergencies and conflicts, "Opportunistic adversaries may seize this moment to compromise networks just to collect data about US communications channels, strategic operations patterns, or national incident preparation and response."

Recommendations to Secure US Critical Infrastructure Against Retaliatory Disruptionware Attacks

The federal government has issued recommendations to US organizations to secure critical infrastructure through the recent CISA, NSA, and FBI advisories and the DoD "Shields Up" Initiative. Below are some additional recommendations from ICIT and our esteemed Fellows.

Be Vigilant Across All Channels

As cyber-hygiene best practices dictate, personnel should be cautious when communicating online and critically evaluate emails, media accounts, and even charity efforts to confirm they are legitimate. Don Maclean, ICIT Fellow and Chief Cyber Security Strategist, DLT, advises, "Bad actors always exploit uncertainty and disruptive events. Be on the lookout for fraudulent charities, phony activism, and phishing attempts. Also, be very careful about consuming and sharing unsubstantiated news and updates in general, but particularly about Ukraine & Russia." Itzik Kotler concurs, "Anytime there is a significant conflict, as we are currently seeing between Russia and Ukraine, it tends to dominate the media and the mindshare of governments and intelligence organizations around the world. This asymmetrical attention ratio can create a window of opportunity for other entities—whether state-sponsored actors, individual cybercriminals, or activist groups—to increase their activities and launch attacks. While it is impossible to make assumptions about the likelihood of these types of attacks, it is important for organizations to stay vigilant against the possibility of attacks from a variety of sources during this time."

Communicate with Key Stakeholders

Now more than ever, a collaborative, whole-of-nation response is needed to stymie adversarial compromise and improve the security and resiliency of our nation's critical infrastructure. Don Maclean agrees, adding, "Be on high alert. Over-Report and Over-Respond." The old "see something, say something" adage has resurged in some estimations of potential cyberthreats; however, that approach is reactive. A stronger, proactive approach is necessary to preempt incidents and proactively begins with communication. While many ISACs and private sector organizations are doing their best to improve information sharing amongst sector stakeholders, a coordinated federal initiative would improve coordination, cooperation, and collaboration amongst the sectors and within each sector. Tim Callahan, ICIT Fellow and SVP & Global CISO, Aflac, adds, "This is a time we need strong support and information flow from US government agencies and the intelligence community. This is a public-private partnership that needs to kick into high gear."

Plan Against the Worse and Hope for the Best

Cyberwarfare is asymmetric and favors the attacker, but we should not presume that the affordance of the less resource-intensive position means that adversaries, especially nation-state-sponsored APTs, are not systematic in the planning of their attack campaigns. Even the most opportunistic attacks proceed from a rough plan. Adversaries that fail to take precautions or sequence their activities fail. Poet Robert Burns asserted, "The best-laid schemes of mice and men often go askew and leave us nothing but grief and pain." When securing critical infrastructure, failure to develop and implement comprehensive cybersecurity defensive strategies can do worse than just cause grief and pain; it could jeopardize national security, may be on the line, or cost peoples' lives. Don Heckman more positively explains, "Experience has taught us that the velocity of cyber-attacks prohibits a 'we'll figure it out when it happens' approach to managing this risk. "Failure to Plan" is not "Planning to Fail" in today's cyber world; a "Failure to Plan" is intentionally ensuring failure."

Strengthen Security Foundations

Pete Slade, ICIT Fellow and CTO, ThreatWarrior, recommends, "Be aware of the heightened threat state and adopt a strengthened security posture. Be prepared and ensure that your incident response plans, cyber resilience plans, business continuity plans, and backups are up to date. Organizations with the ability to do so should begin proactively threat hunting and looking for any indicators of compromise. Investigate any abnormal activity. Ensure your organization is practicing a defense-in-depth strategy. You must use solutions that protect your data, perimeter, endpoints, network, and cloud infrastructure. Check that all software is up to date, and validate any remote access to the organization's network. Now would be a good time to change any credentials and enable multifactor authentication if you aren't already using it." Critical infrastructure organizations should implement security best practices and guidance provided by frameworks such as NIST 800-53 and 800-171. (e.g., Ensure your software is up to date, patched, and appropriately configured. Use multifactor authentication or require all users to change their password especially privileged users, etc.). They should also validate and fortify the security of perimeter defenses, inventory key assets (staff, applications, data, vendors, etc.), identify critical points of failure, and review maximum allowable downtime estimates to manage risk exposure. Russian APTs have a long-documented history of compromising and sabotaging operational technology and legacy systems. It is a matter of national security and resilience for organizations to ensure that operational technology (OT) is segmented from mission-critical information technology (IT) systems and data resources. A baseline security strategy should build from NIST frameworks and CISA recommendations, but it should also leverage known IoCs and TTP. Itzik Kotler explains, "While it is impossible to fully predict the types of attacks that will happen as a result of the current geopolitical situation, we do have a significant amount of data about the Russian state-sponsored threat actors that will likely be active during this time and the attack methods and vulnerabilities they may attempt to exploit based on their previous known activity. While some details about the attacks may change (e.g., the payload), some of the TTPs will remain the same."

Proactively Test Your Networks

Proactively assessing network and system vulnerability and exposure is essential for mitigating low-level attackers and dissuading more sophisticated adversaries. Itzik Kotler expounds, "A key way for organizations to reduce risk of compromise or disruption from these Russian state-sponsored threat actors is to leverage this known information to test their defenses and overall security posture. Adversarial simulation tools are designed to help organizations do that in a safe and systematic way. They provide a "hacker's view" of an organization's security posture by employing the IOCs and TTPs of known threat actors to simulate attacks that provide contextualized results that can be used to optimize security controls, prioritize remediation efforts, and mitigate critical gaps. These tools are most effective if used systematically—consistently testing the maximum amount of IOCs and TTPs— and continuously in order to provide a clear indication of how well an organization is doing at any given point in time and measure the effectiveness of mitigation strategies."

Treat Policies, Procedures, and Guidelines as Security

In addition to hardware and software controls, organizations should increase the resiliency of the people, processes, and policies that comprise the organization. Stan Mierzwa adds, "[Organizations should] use this new threat as an opportunity to review defenses, Information Security policies, and Information Governance programs and update their incident response and disaster recovery plans." Similarly, they gauge third-party incident response plans and procedures and review agreements to clearly outline roles and responsibilities in the event of an incident. Incident Response and Crisis Management capabilities should be updated to include recovery and communications plans, current contact lists, and alternate communication channels.

Test Your Plans!

During the previous global conflict, Winston Churchill allegedly said, "Plans are of little importance, but planning is essential," and Dwight D. Eisenhower separately concurred, "Plans are worthless, but planning is everything." Whether the quotes are accurately attributed is a conflict best left to the annuls of history. In cybersecurity, the sentiment is invaluable. A plan stagnating in a folder is meaningless if personnel are not trained to act on it at the earliest onset of an incident. Just as scenario-based simulations help to prepare defenses and identify security vulnerabilities and gaps, so too do team drills, and gamification exercises help to ensure that staff are trained, equipped, and prepared to recognize and respond to cybersecurity incidents. Acclimating staff to respond in practice is far more important than just having the right steps written down in principle.

Conclusion

Admittedly, it may be dramatic to insinuate that the conflict in Ukraine is going to spark another Cold War; however, the narratives of conflict are subjective and based on known Russian APT activity and strategy, President Vladimir Putin may have never stopped fighting the Cold War even after the Soviet Union fell and the US shifted focus elsewhere. Over the past two decades, in cyberspace and globally, Russia has relied on the Maskirovka strategy in much the same way the Soviet Union did sixty years ago. Regardless of the title applied to the threat, US critical infrastructure must prepare for the eventuality of cyberattacks from Russian state-sponsored advanced persistent threats (APTs) intent on exfiltrating sensitive information, disrupting critical operations, and eroding US national security and resiliency.

Sources

[1] https://www.theguardian.com/business/2022/feb/26/frozen-out-how-the-uks-sanctions-against-russia-will-work

[2] https://www.cnn.com/2022/02/25/business/list-global-sanctions-russia-ukraine-war-intl-hnk/index.html

[3] https://www.bloomberg.com/news/articles/2022-02-25/chinese-state-banks-restrict-financing-for-russian-commodities

[4] https://www.cnn.com/2022/02/22/investing/russia-markets-ruble-economy/index.html

[5] https://fortune.com/2022/02/28/russia-ukraine-sanctions-economy-timeline/

[6] https://www.dailymail.co.uk/news/article-10546799/More-150-senior-Russian-officials-sign-open-letter-condemning-Putins-invasion-Ukraine.html

[7] https://www.bloomberg.com/news/audio/2022-03-03/russian-oligarchs-and-economic-sanctions-radio

[8] https://crsreports.congress.gov/product/pdf/IF/IF11718#page=1&zoom=auto,-150,404

[9] https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_15-06-2021.pdf

[10] https://www.cisa.gov/uscert/ncas/current-activity/2022/02/23/new-sandworm-malware-cyclops-blink-replaces-vpnfilter

[11] https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2935170/nsa-fbi-cisa-release-advisory-on-protecting-cleared-defense-contractor-networks/

[12] https://www.cisa.gov/uscert/ncas/alerts/aa22-057a

[13] https://healthitsecurity.com/news/destructive-malware-used-to-target-ukraine-poses-threat-to-healthcare

[14] https://www.dhs.gov/news/2016/12/30/executive-summary-grizzly-steppe-findings-homeland-security-assistant-secretary

[15] https://www.cisa.gov/uscert/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity

[16] https://www.cisa.gov/uscert/ncas/current-activity/2022/02/24/iranian-government-sponsored-muddywater-actors-conducting

[17] https://www.nbcnews.com/news/world/china-taiwan-ukraine-rcna17964