Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine

by

Jen Weedon

Chapter 8 in
Kenneth Geers (Ed.), Cyber War in Perspective:
Russian Aggression against Ukraine,
NATO CCD COE Publications, Tallinn 2015

CCDCOE
NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

FireEye's Jen Weedon, in Chapter 8, discusses Russia's strategic use of computer network exploitation (i.e. cyber espionage). Today, via the Internet, intelligence agencies can gather information on an industrial scale, which can be used for any purpose, including tactical support to military operations. From a targeting perspective, Weedon discusses strategies for creating a decisive information advantage, 'prepping' a battlefield through denial and deception, and how hackers might even cause real-world physical destruction; and details the technical aspects of suspected Russian cyber operations, including malware samples, hacker tactics, and compromised infrastructure.

CCDCOE

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Disclaimer

This publication is a product of the NATO Cooperative Cyber Defence Centre of Excellence (the Centre). It does not necessarily reflect the policy or the opinion of the Centre or NATO. The Centre may not be held responsible for any loss or harm arising from the use of information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication. Digital or hard copies of this publication may be produced for internal use within NATO and for personal or educational use when for non-profit and non-commercial purpose, provided that copies bear a full citation. Please contact publications@ccdcoe.org with any further queries.

Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine

Jen Weedon

FireEye

1 Introduction

'Cyber attacks' and 'cyber war' are all too often characterised as independent phenomena limited to the cyber domain, somehow distinct from the broader dynamics that define a conflict. An analysis of cyber conflict thus far suggests that such a perceived dichotomy is both inaccurate and unwise. Targeted internet-based assaults cannot be divorced from their underlying geopolitical contexts, and there is small likelihood that a 'cyber war' will ever take place that is limited only to the cyber domain. On the contrary, governments have been shown to use cyber tools and tactics as a broad instrument of statecraft, a tool for coercion, and a complement to kinetic forces in conflict scenarios.

> *Moscow's strategy in Ukraine has included a substantial investment in information operations.*

Moscow's strategy in Ukraine has included a substantial investment in espionage and information operations, relying on the success of integrated cyber operations and computer network exploitation in particular. Russian cyber activities have included cyber espionage, 'prepping the battlefield', selective telegraphing of capabilities, and some hints at destructive activity. Together, these operations have no doubt inexorably contributed to Moscow's advantages over Kyiv, both on the ground and in shaping the conflict's narrative in the public arena. This orchestration should come as no surprise to Russian security analysts, as such an integrated approach is consistent with published Russian military doctrine. Russian strategic thinkers do not consider 'cyber war' (or even the prefix 'cyber') as a distinct concept. Rather, computer network operations are tools to be integrated into broader efforts to maintain political and military dominance in a given theatre and, more broadly, in the domestic and global courts of public opinion.

This chapter will ground strategic thinking on cyber conflict against the systematic cyber espionage that we believe Russia is leveraging in its conflict with Ukraine. Rather than a 'cyber war' waged in a distinct networked domain, Russia's strategy has been to masterfully exploit the information gleaned from its worldwide computer network exploitation campaigns to inform its conduct, purposely distort public opinion, and maintain its dominant position in Ukraine.

The author will examine three types of interrelated Russian cyber operations from a technical and targeting perspective:

1. Computer network exploitation (CNE) to gain a decisive information advantage;
2. 'Prepping the battlefield' via denial and deception; and
3. Limited incidents of cyber disruption and destruction.

2 The Architecture and Artistry of Russia's Strategic Information Theft

Since the start of the Ukraine conflict, security companies have been increasingly tracking, cataloguing, and exposing sustained Russian CNE campaigns. Overall these Russian cyber threat groups have consistently focused on clandestinely stealing intelligence, most likely to give the Russian Government a strategic advantage. The targets of these operations have repeatedly included Ukrainian, European, and U.S. government targets, militaries, international and regional defence and political organisations, think tanks, media outlets, and dissidents. While it is difficult to assess with certainty whether these cyber threat groups are directly tasked or supported by Moscow, there is a growing body of evidence indicating these cyber actors are Russia-based, and that their activities highly likely benefit Moscow.

The security community's ability to detect, track, and ultimately expose Russian cyber operations seems to have improved since the Ukraine conflict began, even relative to overall trends in the industry on exposing threat activity. While determining a direct causation between the conflict in Ukraine and a seemingly marked uptick in observable Russian cyber activity is challenging, the timing is certainly notable. It is exceedingly unlikely that Russian actors only just started conducting aggressive CNE on a global scale, so why has our ability to track and expose their activity appear to have improved? One reason may be that Russia's current national security crisis has increased its government's collections requirements to state-supported hackers, which has in turn accelerated the groups' operational tempo. As a result, it may be more difficult for these actors to modify their tactics, techniques, and procedures (TTPs) on a timely basis, which often results in them tipping their hand.

To shed light on how this sustained information theft is being carried out, the following sections discuss some of the cyber tactics and compromised computer infrastructure that FireEye has associated with two prominent hacker groups that we believe operate from Russia, as well as a summary list of CNE-related activity that is likely being used to give Moscow a geopolitical and military advantage.

3 APT29 ('Advanced Persistent Threat'[1] Group 29)

> *APT29 is a highly capable Russian cyber espionage group with a constantly evolving toolset.*

APT29 is a sophisticated and highly capable Russian cyber espionage group with a diverse, constantly evolving toolset, and talented operators. The group maintains a globally dispersed and intricate attack infrastructure that doubtless requires substantial resources to maintain. APT29's tools often leverage legitimate web services for malware command and control mechanisms, which can make them more difficult to detect because they appear to be benign communications at first glance.

3.1 APT29's Targets: Consistent with Russian State Interests

APT29 typically targets entities to steal information that is closely linked to Russian geopolitical interests and priorities. The group's recent operations suggest it is particularly focused on targets of intelligence value that are related to the Russia-Ukraine crisis and related policy responses. This includes: western governments (particularly foreign policy and defence-related targets); international security and legal institutions; think tanks; and educational institutions.

APT29 usually compromises its victims via socially engineered spear phishing emails– either with malicious email attachments, or through a link to download a malicious file from a compromised website. The group's decoy documents ('lures') often topically align with their targets' interests and work subject matter; this social engineering technique is common and can be very effective. APT29 has also been known to re-purpose and weaponise legitimate documents or information stolen from its previously compromised networks. Example lure topics from legitimate sources include content related to European Union sanctions on Russia, a voicemail

[1] We refer to groups that we assess have a nexus to state sponsorship as 'Advanced Persistent Threat,' or 'APT' groups.

attachment sent from a reporter to a think tank scholar who writes on Russia-Ukraine issues,[2] a PDF report on terrorism, and discussions related to Caucasus regional development and democratisation.[3] APT29 has also used less tailored and pop culture-themed approaches, such as a faked e-fax, and videos of 'Office Monkeys'.[45]

3.2 APT29's Tools and Infrastructure: the Work of Professionals

The complex nature of APT29's malware and infrastructure (requiring significant financial resources and expertise for upkeep), combined with its operational security practices and target sets strongly suggests some level of Russian state sponsorship. Its typical work hours (as defined by active operations in networks the group has compromised) fall within the UTC+3 time zone, which aligns to the time zones of Moscow and St. Petersburg. Furthermore, APT29 has been known to temporarily halt its operations on Russian holidays.[6]

APT29 has been highly active throughout 2015, employing new data theft tools as well as pursuing new targets for stealing information. To maintain operational security, APT29 often configures its malware to activate only at predetermined times, and is adept at using misdirection and obfuscation TTPs[7] that hinder reverse engineering and other means of analysis. One complicated APT29 backdoor, HAMMERTOSS, is highly capable of evading detection, particularly by its ability to mimic the behaviour of legitimate users.[8] HAMMERTOSS accomplishes this stealthiness by leveraging commonly visited websites and web services to relay commands and steal data from victims. The tool works by:

- Checking in and retrieving commands via legitimate web services, such as Twitter and GitHub;
- Using compromised web servers for command and control (C2);
- Visiting different Twitter handles daily and automatically;
- Using timed starts, such as communicating only after a specific date or only during the victim's workweek;
- Obtaining commands via images containing hidden and encrypted data (steganography); and
- Extracting information from a compromised network by uploading files to commonly used cloud storage services.[9]

[2] 'The Connections Between MiniDuke, CosmicDuke and OnionDuke.' January 7, 2015. *F-Secure.* https://www.f-secure.com/weblog/archives/00002780.html.

[3] Graham Cluley. 'MiniDionis: Where a Voicemail Can Lead to a Malware Attack.' July 16, 2015. http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/minidionis-voicemail-malware/.

[4] *Ibid.*

[5] Sergey Lozhkin. 'Minidionis – one more APT with a usage of cloud drives.' *Kaspersky Lab*. July 16, 2015. https://securelist.com/blog/research/71443/minidionis-one-more-apt-with-a-usage-of-cloud-drives/.

[6] FireEye Threat Intelligence, HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group,' July 29, 2015. https://www.fireeye.com/blog/threat-research/2015/07/hammertoss_stealthy.html.

[7] Kurt Baumgartner and Costin Raiu. 'The CozyDuke APT.' *Securelist*. April 21, 2015. https://securelist.com/blog/research/69731/the-cozyduke-apt/.

[8] *Ibid.*

[9] *Ibid.*

APT29 appears to deploy this advanced malware only against high-value networks where it needs not only to steal information but also to maintain persistent access to the victim's environment. In addition, APT29 possesses other advanced, stealthy tools in its toolbox (which include the 'Dukes' malware[10]), and the group is constantly evolving its 'weaponry'.

> *Malware needs not only to steal information but to maintain persistent access to the victim's environment.*

4 APT28 (also known as Tsar Team/Sofacy/Pawn Storm)

APT28 is another Russian cyber espionage group that frequently targets European security organisations, Eastern European governments and militaries, international media outlets, think tanks, defence companies, domestic dissident populations, and entities in the Caucasus. This list is not exhaustive.[11] The following table summarises some of what currently know about APT28.[12]

Like APT29, APT28 works in a highly professional manner worthy of its 'advanced persistent threat' moniker. Security researchers believe its malware is written in a Russian language development environment, and that it has been systematically updating its tools, some of which are also able to target mobile devices[13] since 2007.

One way to appreciate the sophisticated nature of APT28 is through its exploitation of 'zero-day' vulnerabilities; that is, previously undiscovered and unpatched vulnerabilities. For example, in early 2015, APT28 likely exploited two zero-day vulnerabilities in Adobe Flash and Microsoft Windows in an attack against a government contractor.[14] In a separate incident in July 2015, APT28 rapidly integrated into its operations multiple zero-day vulnerabilities exposed in the highly public breach of the Italian exploit dealer Hacking Team.[15]

[10] 'Duke APT group's latest tools: cloud services and Linux support.' July 22, 2015. *F-Secure*. https://www.f-secure.com/weblog/archives/00002822.html; Kurt Baumgartner, Costin Raiu. 'The CozyDuke APT.' *Kaspersky Lab*. April 21, 2015. https://securelist.com/blog/69731/the-cozyduke-apt/; Brandon Levene, Robert Falcone and Richard Wartell. 'Tracking MiniDionis: CozyCar's New Ride Is Related to Seaduke.' *Palo Alto Networks*. July 14, 2015.

[11] 'APT28: A Window into Russia's Cyber Espionage Operations?' FireEye Blog.October 27, 2014. https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html.

[12] *Ibid.*

[13] Dune Lawrence and Michael Riley. 'Hackers Target Hong Kong Protesters via iPhones.' *Bloomberg Business*. October 1, 2014. http://www.bloomberg.com/bw/articles/2014-10-01/hackers-target-hong-kong-protesters-via-iphones.

[14] FireEye Labs. 'Operation RussianDoll: Adobe & Windows Zero-Day Exploits Likely Leveraged by Russia's APT28 in Highly-Targeted Attack.' April 18, 2015. https://www.fireeye.com/blog/threat-research/2015/04/probable_apt28_useo.html.

[15] Jonathan Leathery. 'Microsoft Office Zero-Day CVE-2015-2424 Leveraged By Tsar Team..' *iSight Partners.* July 15, 2015. http://www.isightpartners.com/2015/07/microsoft-office-zero-day-cve-2015-2424-leveraged-by-tsar-team/.

Malware	Targeting	Russian Attributes
Evolves and Maintains Tools for Continued, Long-Term Use • Uses malware with flexible and lasting platforms • Constantly evolves malware samples for continued use • Malware is tailored to specific victims' environments, and is designed to hamper reverse engineering efforts • Developed in a formal code development environment **Various Data Theft Techniques** • Backdoors using HTTP protocol • Backdoors using victim mail server • Local copying to defeat closed/air gapped networks	**Georgia & the Caucasus** • Ministry of Internal Affairs • Ministry of Defence • Journalist writing on Caucasus issues • Kavkaz Center **Eastern European Governments & Militaries** • Polish Government • Hungarian Government • Ministry of Foreign Affairs in Eastern Europe • Baltic Host exercises **Security-related organisations** • NATO • OSCE • Defense attaches • Defense events and exhibitions	**Russian Language Indicators** • Consistent use of Russian malware over a period of six years • Lure to journalist writing on Caucasus issues suggests APT28 understands both Russian and English **Malware Compile Times Correspond to Work Day in Moscow's Time Zone** • Consistent among APT28 samples with compile times from 2007 to 2014 • The compile times align with the standards workday in the UTC +4 time zone, which includes major Russian cities such as Moscow and St. Petersburg

Figure 1-1 – APT28 Activities

5 A Crowded Playing Field: Additional Examples of Russian CNE

Numerous cyber security companies have characterised a range of suspected Russian state-sponsored cyber activity and malware. Overall, there are recurring themes in their findings, which suggests that Russian CNE campaigns are based on consistent taskings. Multiple cyber espionage campaigns ongoing across the globe since at least 2007 (and no doubt much earlier) has probably given these actors a considerable information advantage. A few examples are as follows.

> *Russian CNE campaigns are based on consistent taskings.*

In September 2015, Kaspersky Labs published research exposing multiple Russian APT groups 'using and abusing' satellite-based internet links (particularly IP addresses in Middle Eastern and African countries) to hide their operational command and control. This infrastructure likely enables a high degree of operational security. One of the groups using this tactic is the same group behind the Snake/Uroburos/Turla malware, thought to be related to the infamous Agent. BTZ, which was used to penetrate U.S. military networks as early as 2008. Kaspersky's report outlined a specific campaign targeting government, embassies, military entities, universities, research organisations, and pharmaceutical companies worldwide.[16]

In August 2015, a group of security researchers described the enterprise-like effort behind the Gameover ZeuS malware and its prolific and FBI-sought author Evgeniy Mikhailovich Bogachev (a.k.a. 'Slavik'). The malware was used to facilitate both cyber crime and espionage. Further, the researchers discovered commands in the malware indicating that the actors sought to gather classified information from victims in Ukraine, Georgia, and Turkey,[17] suggesting a link between Russia's cyber crime syndicates and government espionage actors.

In late 2014, researchers exposed a long-active Russian group called 'Sandworm,' whose victims included NATO, the Ukrainian Government, EU governments, energy and telecommunications firms, and an American academic organisation. The group used zero-day exploits and infected victims through a variety of means including malicious PowerPoint attachments and the BlackEnergy toolkit.[18]

Between 2013 and 2014, actors using the Snake/Uroburos/Turla malware targeted Ukrainian computer systems in dozens of cyber operations launched by 'committed and well-funded professionals'.[19] This malware is highly complex, reistant to countermeasures, and thought to have been created in 2005.[20]

Since 2013, 'Operation Armageddon' – a Russian cyber espionage campaign allegedly targeting Ukrainian government, law enforcement, and military officials – has likely helped provide a military advantage to Russia vis-à-vis Ukraine from secrets systematically gathered from cyber espionage. [21]

In 2012, suspected Russian actors reportedly used the Wipbot and Snake backdoors for long-term cyber espionage. The actors leveraged legitimate (but compromised) websites to systematically deliver malware, particularly to victims in Eastern Europe.[22]

6 Prepping the Battlefield

The cyber espionage activity previously described entails the penetration and exploitation of networks in order to steal sensitive information. However it is important to note that the network access required for CNE can, depending on

[16] Stefan Stanase. 'Satellite Turla: APT Command and Control in the Sky.' *Securelist Blog.* September 9, 2015. https://securelist.com/blog/research/72081/satellite-turla-apt-command-and-control-in-the-sky/.

[17] Michael Sandee. 'GameOver Zeus. Backgrounds on the Badguys and the Backends.'*FoxIT Whitepaper*. https://www.fox-it.com/en/files/2015/08/FoxIT-Whitepaper_Blackhat-web.pdf.

[18] 'iSIGHT discovers zero-day vulnerability CVE-2014-4114 used in Russian cyber-espionage campaign.' *iSight Partners*, October 14, 2014. http://www.isightpartners.com/2014/10/cve-2014-4114/.

[19] 'The Snake Campaign.' *BAE Systems.* 2014.www.baesystems.com/ai/snakemalware.

[20] 'Ukraine attacked by cyberspies as tensions escalated in recent months.' *Associated Press*. March 9, 2014. http://www.theguardian.com/world/2014/mar/09/ukraine-attacked-cyberspies-tensions-computer.

[21] Lookingglass. 'Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare – CTIG Report.' April 28, 2015. https://lgscout.com/operation-armageddon-cyber-espionage-as-a-strategic-component-of-russian-modern-warfare-ctig-report/.

[22] Symantec Security Response. 'Turla: Spying tool targets governments and diplomats.' August 7, 2014. http://www.symantec.com/connect/blogs/turla-spying-tool-targets-governments-and-diplomats.

the intent of the attacker, also be used for disruptive or destructive CNA, including what military professionals call ‘preparation of the battlefield’ for potential conflict scenarios. [23,24] The cyber backdoors used to access environments illicitly or lay low and maintain persistence could also be used to enable future attacks.

Extensive preparation of the battlefield is consistent with Russian strategic thinking. During the Cold War, the Soviet Union developed highly detailed maps of U.S. and European cities – all the way down to individual buildings, terrain, and weather. This information would be invaluable in the event of invasion or occupation, as in Crimea.[25] Russian ‘mapping’ of an adversary’s cyber infrastructure is in principle the same concept. Computer networks, however, are harder to map: like living organisms, they constantly evolve. Therefore, today’s map might not be good tomorrow, which is why Russian malware implants like HAMMERTOSS are designed to sustain clandestine access.

> *Extensive preparation of the battlefield is consistent with Russian strategic thinking.*

6.1 Preparing for Attack?

Is Russia preparing for future cyber attacks on Western critical infrastructure? This is difficult to prove, but the Sandworm group has reportedly targeted supervisory control and data acquisition (SCADA) equipment, which is used in industrial and critical infrastructure settings, with the BlackEnergy toolkit.[26] The victims were production systems, not vendor-owned prototypes or systems that contained financial information, intellectual property, or political intelligence. Given the targets seemed to be production systems, there would likely be no benefit from an espionage perspective to infect these systems. Rather, the actors using the malware may have been looking for weaknesses to exploit in a future disruptive scenario. In addition, the use of a crimeware toolkit offers a degree of anonymity or plausible deniability for actors with more destructive purposes.

[23] Jen Weedon and Jacqueline Stokes. ‘Security in an Era of Coercive Attacks.’ *FireEye Executive Perspectives Blog*. May 14, 2015. https://www.fireeye.com/blog/executive-perspective/2015/05/security_in_an_erao.html.

[24] In the U.S., CNE and CNA may be carried out by different government agencies operating under different authorities, but not all countries will have this same dichotomy.

[25] Nick Ballon. ‘Inside the Secret World of Russia’s Cold War Maps.’ *Wired*. http://www.wired.com/2015/07/secret-cold-war-maps/

[26] Kyle Wilhoit and Jim Gogolinski. ‘Sandworm to Blacken: The SCADA Connection.’ October 16, 2014. http://blog.trendmicro.com/trendlabs-security-intelligence/sandworm-to-blacken-the-scada-connection/.

7 Deception and Telegraphing Intent: APT28 and TV5Monde

Russia has a long history of using information operations and deception to create confusion or sow panic to ultimately create favourable conditions for their activity.[27] This tactic has simply evolved for the internet era to include online misinformation campaigns and propaganda, and extensive internet trolling. One of the more remarkable incidents this year included APT28's possible use of false flag operation against a French TV station.

In April 2015, hackers claiming to be the Islamic State-affiliated 'Cyber Caliphate' hacked France's *TV5 Monde* channel, shutting off transmissions for eighteen hours, and posting Islamic State propaganda on the *TV5 Monde's* Facebook and Twitter accounts. The attack also apparently resulted in significant damage to the channel's broadcasting infrastructure.[28]

This incident generated enormous publicity and speculation over Cyber Caliphate's apparently growing capabilities and intent. However, technical analysis of the attackers' network infrastructure (such as the IP block hosting the Cyber Caliphate's website, its server, and registrar)[29] as well as some other sensitive source reporting related to the malware used suggests that Russia's APT28 was in fact the more likely perpetrator of this attack. French Police concurred with this conclusion, stating 'Russian hackers linked to the Kremlin' may have been responsible'.[30] In a similar vein, *The New York Times* reported that a Russian organisation known as the 'Internet Research Agency' had conducted systematic online trolling and hoaxes in the U.S., including a spoofed Islamic State attack against a Louisiana chemical plant on the anniversary of 9/11.[31]

If APT28 (or another Russian hacker group) conducted these attacks, what were their motivations? There are a number of plausible scenarios, including:

- Russian actors may have been displeased at *TV5 Monde* coverage of the Ukraine conflict, and this was an act of retribution;
- Russian actors wanted to distract attention from the Kremlin's actions in Ukraine by shifting the focus of Western national security planners to the Islamic State;

[27] Roland Heickerö. 'Emergin Cyber Threats and Russian Views on Information Warfare and Information Operations.' FOI, Swedish Defence Research Agency. March 2010. http://www.foi.se/ReportFiles/foir_2970.pdf.

[28] Cale Guthrie Weissman. 'France: Russian hackers posed as ISIS to hack a French TV broadcaster.' *Business Insider*. June 11, 2015. http://www.businessinsider.com/new-discovery-indicates-that-russian-hackers-apt28-are-behind-the-tv5-monde-hack-2015-6.

[29] Sheera Frankel. 'Experts Say Russians May Have Posed As ISIS To Hack French TV Channel.' Buzzfeed. June 9, 2015. http://www.buzzfeed.com/sheerafrenkel/experts-say-russians-may-have-posed-as-isis-to-hack-french-t#.wg4BeJ6xDP ; Eamon Javers. 'These cyberhackers may not be backed by ISIS.' *CNBC*. July 14, 2015. http://www.cnbc.com/2015/07/14/these-cyber-hackers-not-backed-by-isis.html.

[30] Joseph Menn and Leigh Thomas. 'France probes Russian lead in TV5Monde hacking: sources'. *Reuters*. June 10, 2015. http://www.reuters.com/article/2015/06/10/us-france-russia-cybercrime-idUSKBN0OQ2GG20150610.

[31] Adrian Chen. 'The Agency.' *New York Times*. June 2, 2015. http://www.nytimes.com/2015/06/07/magazine/the-agency.html?_r=0.

- Russian actors actively sought exposure as the perpetrators, and by doing so, telegraph that they were both willing and capable of pulling off such a scheme, while refining their ability to disrupt and destroy digital media broadcasting capabilities.

8 'Cyber War' in Ukraine – Not Much to See Here

There have been significant cyber espionage operations directed against victims related to Russia's strategic interests, particularly in regards to the situation in Ukraine. However we have not seen high profile, coercive and damaging attacks similar to those waged on Estonia in 2007 or Georgia in 2008.

> *We have not seen coercive and damaging attacks similar to Estonia or Georgia.*

The publicly reported examples of CNA in Ukraine mostly include Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks designed to undermine Ukraine's telecommunications infrastructure. For the attackers, these were likely a low-risk way to disrupt the flow of information within the Ukrainian national security space, as well as a way to selectively and temporarily silence specific voices online. Some of the known incidents are listed below:

- November 2013: Russian hackers reportedly defaced and DDoS'ed the websites of several Ukrainian TV stations, news outlets, and politicians.[32]
- February 2014: Russian troops allegedly tampered with Ukraine's fibre optic cables and raided *Ukrtelecom*, which stated that it had 'lost the technical capacity to provide connection between the peninsula and the rest of Ukraine and probably across the peninsula, too'.[33] In Crimea, mobile, landline, and internet access were all affected.
- March 2014: As Russian troops entered Crimea, the main Ukrainian Government website was shut down for nearly 72 hours,[34] many other official government and media websites were targeted in DDoS attacks,[35] and the cell phones of many Ukrainian parliamentarians were 'hacked'.[36]

[32] 'Hromadske.tv under DDoS-attack.' *Institute of Mass Information*. November 26, 2013. http://imi.org.ua/en/news/42266-hromadsketv-under-ddos-attack.html.

[33] 'Ukrtelecom's Crimean sub-branches officially report that unknown people have seized several telecommunications nodes in the Crimea.' February 28, 2014. http://en.ukrtelecom.ua/about/news?id=120467.

[34] 'Ukraine says communications hit, MPs phones blocked.' *Reuters*. March 4, 2014. http://www.reuters.com/article/2014/03/04/ukraine-crisis-cybersecurity-idUSL6N0M12CF20140304.

[35] Cornelius Rahn, Ilya Khrennikov and Aaron Eglitis. 'Russia-Ukraine Standoff Going Online as Hackers Attack.' *Bloomberg*. March 6, 2014. http://www.bloomberg.com/news/articles/2014-03-05/russia-ukraine-standoff-going-online-as-hackers-attack.

[36] Peter Bergen and Tim Maurer. 'Cyberwar hits Ukraine.' *CNN*. March 7, 2014. http://www.cnn.com/2014/03/07/opinion/bergen-ukraine-cyber-attacks/.

- May 2014: the pro-Russian hacktivist group *CyberBerkut* claimed responsibility for a breach of the systems of Ukraine's Central Election Commission with malware that would have deleted the results of the presidential election. However, Ukraine's Security Service (SBU) removed the malware and replaced the election software prior to the vote.[37]

Outside of these limited publicly reported incidents, it appears that the Kremlin has either not needed or not chosen to engage in extensive overt CNA during this conflict. One reason for this could be that Moscow wants to avoid the international criticism that followed its alleged cyber operations in the 2008 war in Georgia, and in Estonia in 2007. Instead, Moscow seems to be using more narrowly focused, limited operations in support of strategic state objectives, primarily via sustained cyber espionage rather than widespread attacks.

9 Information War, Not Cyber War

In the Russia-Ukraine conflict, computer network operations have not been limited to trite notions of 'cyber war.' Rather, an examination of the sustained tensions suggests that this has been a war waged with and by the strategic theft and manipulation of information, and not extensive application of destructive cyber attacks. Russia's unrelenting cyber espionage campaigns over time, and against so many targets, have no doubt given it a considerable advantage in understanding, anticipating, and in some instances outmanoeuvring its enemies. This approach may have rendered DDoS and other destructive attacks less necessary or preferable.

> *This has been a war waged with and by the strategic theft and manipulation of information.*

While we do not always have definitive attribution, the malicious cyber tools and attacker infrastructure used by these suspected Russian government-backed actors in many ways mimic what we would expect from Russian intelligence operatives, defined by stealth, artistry in tradecraft, and a high regard for operational security. Yet, as mirrored in Russia's real-life politics, some of the actors also appeared flippant and even brazen at times, characteristics that could reflect an absence of fear of getting caught or any sense of effective deterrence. In this sense, such behaviour will no doubt continue, and it remains of the utmost important to anticipate and defend against this activity, both for short-term network security and for long-term international stability.

[37] "Cyber-attack' cripples Ukraine's electronic election system ahead of presidential vote.' *RT*. May 24, 2014. http://rt.com/news/161332-ukraine-president-election-virus/.