RUSSIA STUDIES CENTRE
AT THE HENRY JACKSON SOCIETY

# Putin’s Cyberwar: Russia’s Statecraft in the Fifth Domain

Russia Studies Centre
Policy Paper No. 9 (2016)

Dr Andrew Foxall

The Henry Jackson Society
May 2016

THE HENRY JACKSON SOCIETY
DEMOCRACY·FREEDOM·HUMAN RIGHTS

# Summary

- Events over the past two years, not least the annexation of Crimea and military intervention in Syria, have demonstrated that Russia has returned to an aggressive foreign policy. The capabilities that Russia has displayed over this period have caught the West off guard.

- Russia's distinctive approach to war in Ukraine has highlighted the Kremlin's capacity for information warfare. There is nothing fundamentally new about the techniques and methods employed by Russia, even if the technologies that enable them are. This is the case with cyberwarfare, where the development of the Internet has facilitated broader and much longer-term information warfare aims.

- Over the past decade, Russia has demonstrated both a greater capacity of its cyberwarfare capabilities and an increasing willingness to use them. Russia has employed cyberwarfare for a variety of purposes – including to dismiss and distort information; to disorient nation-states; and, to distract from, or support, conventional military activities. Russia, or hackers close to the Russian state, have attacked nation-states, industrial plants, financial institutions, government departments, media outlets, and other Western targets.

- One specific military development is particularly worrisome. Russia is the only country to date to have combined cyberwarfare with conventional warfare. In its war with Georgia, in 2008, Russia's ground offensives were accompanied by widespread cyberattacks targeting government websites. In its war with Ukraine, since 2014, Russia's hybrid warfare has included cyberattacks not only on government and media websites, but also on energy infrastructure.

- This trend with Russia's cyberwarfare, as with its conventional warfare, is only likely to continue – the more Russia develops its capabilities, the more aggressive and confident it will become. In contrast to Russia's neighbours, who must consider and plan for the threat of military attack and invasion by Russia, Western countries must plan for the threat of Moscow's ongoing subversion and destabilisation.

- The West should take a tougher approach to Russia's cyberwarfare; investing resources in intelligence gathering, addressing weaknesses that facilitate the Kremlin's activities, and financing an education programme for Internet security.

# 1. Introduction

Russia is at war with the West. Not only in a conventional sense, although given the Kremlin's brazen acts over the last decade – the murder of Alexander Litvinenko in 2006, the invasion of Georgia in 2008, the annexation of Crimea in 2014 and the destabilisation of Ukraine since 2014 – you could be forgiven for thinking otherwise. Russia is also waging a covert war, characterised by scarcely believable, but nevertheless plausible, deniability.

It is a war guided by old-school Soviet-style thinking, with strategies that have been adopted to fit new technologies and whose weapons are very much of the twenty-first century. It is a war that reflects a realisation by the Kremlin that in the age of the Internet there are easier and safer ways of attacking the enemy than dropping bombs or firing bullets. It is a war in which computers and keyboards rather than guns and tanks are the materiel. After land, sea, air, and space, it is a war in the fifth domain. It is cyberwarfare.[1]

Russia, of course, is not unique in waging cyberwarfare against the West. But it is the only country to date to have combined cyberwarfare with conventional warfare. In March 2014, in the midst of Russia's annexation of Crimea, the main Ukrainian government website[2] was taken offline for about 72 hours following a cyberattack.[3] When the European Parliament and Commission began to criticise Russia's actions on the peninsula, in April 2014, its systems too were hit.[4] Six years earlier, in August 2008, Russia's invasion of Georgia had been accompanied by widespread cyberattacks against Tbilisi by pro-Russian hackers.

As far as the Kremlin is concerned, geeks and hackers now rank alongside soldiers and spies as weapons of the state.

This policy paper examines Russia's cyberwarfare with the West. It seeks to answer two questions in light of this: What are Russia's capabilities? And what can or should the West do about them? The paper begins by defining what is meant by the term 'cyber', before moving on to situate cyberwarfare within the broader context of Russia's foreign policy. Next, it outlines a number of incidents in which Russia, or hackers close to the Russian government, has waged cyberwar. After considering what Russia's actions mean, and what the West has done to defend itself thus far, the paper concludes with a review of policy implications for the UK, and for the West as a whole, of Russia's cyberwarfare.

[1] It is not just the West that is targeted, either; the Kremlin's domestic enemies have also been hit. On the day of Russia's 2011 parliamentary election, for example, coordinated cyberattacks crashed the websites of many of the country's liberal media outlets. Internet trolls have reportedly been paid to smear the opposition leader Alexey Navalny. See, Soldatov, A. and Irina Borogan, *The Red Web: The Struggle Between Russia's Digital Dictators and The New Online Revolutionaries* (Public Affairs; New York, 2015).

[2] The website is www.kmu.gov.ua, last visited: 6 May 2016.

[3] Polityuk, P. and Jim Finkle, 'Ukraine says communications hit, MPs phones blocked', *Reuters*, 4 March 2014, available at: http://uk.reuters.com/article/uk-ukraine-crisis-cybersecurity-idUKBREA231QN20140304, last visited: 6 May 2016.

[4] Many of the attacks featured a modified version of the Russia-designed 'BlackEnergy', which is a kind of malware known as a Trojan horse that remotely takes over computers in order to carry out Distributed Denial of Service, or DDoS, attacks. See, Kovacs, E. 'Ukraine Accuses Russia of Hacking Power Companies', *Security Week*, 30 December 2015, available at: http://www.securityweek.com/ukraine-accuses-russia-hacking-power-companies, last visited: 6 May 2016.

## 2. A Note on 'Cyber' and 'Cyberwarfare'

A discussion of cyberwarfare is complicated by widespread disagreement over how to define the term 'cyber' and over what exactly constitutes 'cyberwarfare'. 'Cyber' is not – or at least, should not be considered to be – synonymous with the Internet. Instead, according to the leading cyber expert Martin Libicki, it is better to think of 'cyber' as involving the "command and control of computers".[5] Thus, argues the academic Dr Andrew Futter, cyberattacks can be defined as "all efforts to disrupt, deny, degrade, distort or destroy the information that they rely upon, store, process and generate".[6] For some, most cyberattacks are examples of vandalism or hooliganism, and such cyberattacks only become cyberwarfare depending on who carries out the attacks and what their motives are.[7] For others, a cyberattack must take place alongside conventional military operations for it to qualify as 'cyberwar'. Not everyone agrees, however. Others still argue that future wars will be waged in cyberspace, displacing conventional military operations altogether.

Why does this matter? Under international law, a country that considers itself the victim of an act of war – including cyberwar – has the right to defend itself. And members of an alliance with mutual defence obligations, such as NATO, may be duty bound to respond to an attack on any of their members.

## 3. Cyberwar and Russian Foreign Policy

On 1 March 2014, the day after Russia's "little green men" had appeared in Crimea, Western security experts were expecting Ukrainian government websites to be hit by massive Distributed Denial of Service, or DDoS, attacks. Their expectations were based on a sound understanding of Russia's foreign policy.

Over the past 16 years, Russia has pursued an increasingly assertive foreign policy, designed to dominate its neighbouring states and bring them back into its sphere of influence. This process has run in parallel with Russia's growing confidence and strength, initially underpinned by huge energy revenues. Notwithstanding a brief period of optimism for cooperation with the West following the 9/11 attacks in the United States, Russia has acted with hostility toward its western neighbours. Economic embargoes, financial subversion, energy cut-offs, and social destabilisation are some of the levers Russia has used.

2007 marked a significant escalation in this, when a series of attacks was launched from Russia on Estonia in response to the Baltic country's decision to relocate a Soviet-era statue from the centre of the capital, Tallinn. The following year, when Russia went to war with Georgia in August 2008, Moscow's ground offensives against Tbilisi were accompanied by major cyberattacks targeting the country's government websites and Internet infrastructure.

[5] Futter, A. 'Is Trident safe from cyber attack?', European Leadership Network, February 2016, available at: http://www.europeanleadershipnetwork.org/medialibrary/2016/02/04/d2106a19/Is%20Trident%20safe%20from%20cyber%20attack.pdf, last visited: 6 May 2016.

[6] Ibid.

[7] 'Marching off to cyberwar', *The Economist*, 4 December 2008, available at: http://www.economist.com/node/12673385, last visited: 6 May 2016.

In the years since, Russia has conducted cyberattacks on Western states. Hackers close to the Kremlin have attacked a French television network, a German steelmaker, the Polish stock market, and the US State Department. Cyberwarfare has solidified, in effect, as a tool of Russian statecraft.

For a while, the Ukraine conflict developed along the same lines as the Georgian war. On 3 March, the Ukrainian information agency, UNIAN, reported that its website had been hit by a powerful DDoS attack, causing it to go offline temporarily. Over the following days, other websites suffered the same fate: Ukraine's National Security and Defence Council, the Crimean Supreme Council, and the Crimean independence referendum websites were hit.[8] But the large and much-feared cyberattacks did not take place. Or at least, not as expected. Rather than massive DDoS attacks, a tidal wave of anti-Ukrainian disinformation was spread through social networks and social media.

That Russia responded to the Ukrainian conflict by unleashing propaganda on Ukraine rather than cyberwar should not be read as a departure from the norm for Russia's relations with its neighbours. Nor should it be read as signifying that Russia had retreated from the fifth domain. Instead, it reflected certain particularities about the situation in Ukraine: a large population in both countries speaks Russian and the Russia-based *Vkontakte* was the most popular social network in Ukraine, making it relatively straightforward for the Kremlin to spread disinformation among Ukraine's citizenry.

As a matter of fact, Russia did continue to engage in cyberwar during its war against Ukraine, but it did so toward the West. On 15 March, for example, DDoS attacks disrupted access to some NATO websites.[9] Those responsible were a pro-Russian Ukrainian group called *Cyber Berkut*; a name that clearly echoes the title of Ukraine's *Berkut* riot police.[10]

Above all else, Russia's campaign against Ukraine demonstrated that the Kremlin places as much emphasis on its information operations as it does on its conventional military operations. And these information operations combine electronic warfare, psychological operations (psy-ops), and cyberwarfare. Each is part of the much broader process of what Peter Pomerantsev and Michael Weiss have called the Kremlin's "weaponisation of information".[11]

# 4. Russia's Targets

Russia's cyberwarfare against Ukraine did not fully demonstrate either its capabilities or its reach. However, Russia's actions toward the West over the past decade demonstrate beyond doubt that it has significant cyber capabilities. During this period, Russia has targeted a variety of individuals and entities, including government agencies as well as some financial and energy firms, on an alarming regular basis.

[8] Daly, J. C. K. 'Ukrainian–Russian Dispute Moves Into Cyberspace', *Eurasia Daily Monitor*, Volume 11 Issue 53, 20 March 2014, available at: http://www.jamestown.org/single/?tx_ttnews[tt_news]=42123&no_cache=1#.VyhrS0d_diY, last visited: 6 May 2016.
[9] Including the main website, www.nato.int, last visited: 6 May 2016.
[10] Croft, A. and Peter Apps, 'NATO websites hit in cyber attack linked to Crimea tension', *Reuters*, 16 March 2014, available at: http://www.reuters.com/article/us-ukraine-nato-idUSBREA2E0T320140316, last visited: 6 May 2016.
[11] Pomerantsev, P. and Michael Weiss, 'The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money', A Special Report presented by The Interpreter, a project of the Institute of Modern Russia, available at: http://www.interpretermag.com/wp-content/uploads/2014/11/The_Menace_of_Unreality_Final.pdf, last visited: 6 May 2016. See also Nimmo, B. 'Anatomy of an info-war: How Russia's propaganda machine works, and how to counter it', GlobSec Policy Institute, 15 May 2015, available at: http://www.cepolicy.org/publications/anatomy-info-war-how-russias-propaganda-machine-works-and-how-counter-it, last visited: 6 May 2016.

According to Richard Burr, Chairman of the US Senate Intelligence Committee, it is unclear whether the current Russia–West standoff over Ukraine has led to a demonstrable rise in Russian cyberattacks against the West precisely because the number of such attacks is already so high. Ian West, head of cyber security at NATO's Communications and Information Agency, has estimated that, each week, NATO deals with around 200 million suspicious cyber events, of which between 250 and 300 are cyberattacks – although he did not specify from where the attacks came.[12]

### *4.1 Nation-states*

In August 2008, Russia went to war with Georgia over the breakaway territories of Abkhazia and South Ossetia. After Russia quickly defeated Georgia's army and as its tanks advanced deep into Georgia, another force was mobilising. Alongside the Russian invasion of its territory, Georgia was subjected to a series of cyberattacks. Several pro-Russian websites made available software and instructions that allowed anybody who downloaded them to contribute to DDoS attacks. One website, called StopGeorgia, even provided a list of target websites.[13] The damage done by such open-source cyberwarfare was significant: several government websites were compromised, leading the government to hosting its sites in the US, while Georgia's Ministry of Foreign Affairs was forced to move to a BlogSpot account, in order to disseminate real-time information.

Weeks before Russia's invasion, in what may have been a dress rehearsal for the cyberwar once the shooting had started, a number of websites in Georgia – including that of President Mikheil Saakashvili – suffered from pro-Russian cyberattacks.[14]

Two months before Russia's war with Georgia, Lithuania was hit by a cyberattack. In June, Lithuanian lawmakers voted to ban the public display of Nazi German and Soviet symbols. Some 300 websites, including those of public institutions such as the National Ethics Body and the Securities and Exchange Commission, as well as a series of private companies, found themselves under cyberattack. The content on their websites was replaced with images of the Soviet flag alongside anti-Lithuanian slogans.[15]

There is no conclusive evidence that the attacks against Georgia or Lithuania were executed or sanctioned by the Russian government – though there is no evidence that it tried to stop them, either. Analysts who have researched the attacks suggest that they were the work of a St. Petersburg-based criminal gang known as the Russian Business Network, or RBN.[16]

A year earlier, in April 2007, Estonia had provoked the Kremlin with its decision to move a Soviet war memorial out of the centre of the capital, Tallinn. After an anti-Estonian campaign in Russia's domestic and international press, a series of DDoS attacks was launched on the websites of the Estonian government, parliament, ministries, broadcasters, and newspapers. The servers of the country's banks were hacked, forcing them to close down all but essential operations and move to

[12] Borger, J. '"Trident is old technology": the brave new world of cyber warfare', *The Guardian*, 16 January 2016, available at: https://www.theguardian.com/technology/2016/jan/16/trident-old-technology-brave-new-world-cyber-warfare, last visited: 6 May 2016.

[13] 'Marching off to cyberwar', *The Economist*, 4 December 2008, available at: http://www.economist.com/node/12673385, last visited: 6 May 2016.

[14] Markoff, J. 'Before the Gunfire, Cyberattacks', *The New York Times*, 12 August 2008, available at: http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0, last visited: 6 May 2016.

[15] Adomaitis, N. 'Lithuanian tax office website hit by cyber attack', *Reuters*, 21 July 2008, available at: http://www.reuters.com/article/lithuania-web-attacks-idUSMAR14153920080721, last visited: 6 May 2016.

[16] On RBN, see Warren, P. 'Hunt for Russia's web criminals', *The Guardian*, 15 November 2007, available at: https://www.theguardian.com/technology/2007/nov/15/news.crime, last visited: 6 May 2016.

proxy servers in Lithuania.[17] Without a shot being fired, the country's entire financial infrastructure was forced into exile.

For a number of years, Russian government officials habitually denied any responsibility for these attacks. But in December 2011, Konstantin Goloskokov, a prominent figure in the pro-Kremlin *Nashi* youth movement, in an interview with the *Financial Times*, admitted that he and some of his associates had launched the 2007 attacks on Estonia.[18]

### *4.2 Government Agencies*

Sometime around 25 July 2015, the unclassified email system of the US Pentagon's Joint Chiefs of Staff was subjected to a "sophisticated cyberattack".[19] Some 4,000 military and civilian personnel who work for the Joint Chiefs of Staff were affected, and the system was shut down and taken offline for nearly two weeks. The system had been infiltrated by malware that rapidly gathered massive amounts of data and equally rapidly distributed all the information to thousands of accounts on the Internet. Only unclassified accounts and emails were hacked, and no classified information was compromised.

The incident was not a one-off. A month earlier, in June, the tax returns of more than 100,000 people were stolen from the Internal Revenue System, in a cyberattack.[20] Earlier still, in March, the State Department revealed that hackers had been targeting its unclassified email system for much of the previous 12 months.[21] Individuals close the Department described the intrusion as the "worst ever" cyberattack against a federal agency. So deep had the intrusion been that the hackers had obtained email correspondence from individuals within the White House with whom President Obama regularly communicated.[22] And so severe had it been that the Department had, in November 2014, shut down its email system over a weekend to try to improve security and block the intruders.

Russia has strongly denied its involvement in these cyberattacks, despite evidence that suggests otherwise.[23] But it is not only government agencies in the US that have been targeted.

On 17 July 2014, Malaysia Airlines Flight 17 was destroyed over eastern Ukraine while on a scheduled flight from Amsterdam to Kuala Lumpur. All 298 people on board were killed. Two months after the disaster, an international investigation into the crash was launched, led by the Dutch Safety Board. Shortly before the Board released its detailed report, on 13 October 2015, it was hit by a cyberattack.[24] The attack lasted for several days, eventually ending after the report had

[17] At the same time, mass text messages were sent from an anonymous source to Estonia's Russian-speaking minority population, telling them to drive very slowly through the city centre at a certain time of day. The drivers kept moving, so technically no crime was committed, but it brought Tallinn to a virtual standstill. Then the telephone numbers of vital government services all started ringing at once, nonstop, as they were swamped by robot calls.

[18] Clover, C., 'Kremlin-backed group behind Estonia cyber blitz', *Financial Times*, 11 March 2009, available at: http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html#axzz46TAOpQxb, last visited: 6 May 2016.

[19] Kube, C. and Jim Miklaszewski, 'Russia hacks Pentagon computers: NBC, citing sources', NBC News, 6 August 2015, available at: http://www.cnbc.com/2015/08/06/russia-hacks-pentagon-computers-nbc-citing-sources.html, last visited: 6 May 2016.

[20] Frates, C., 'IRS believes massive data theft originated in Russia', *CNN*, 5 June 2015, available at: http://edition.cnn.com/2015/05/27/politics/irs-cyber-breach-russia/, last visited: 6 May 2016.

[21] Perez, E. and Shimon Prokupecz, 'Sources: State Dept. hack the "worst ever"', *CNN*, 10 March 2015, available at: http://edition.cnn.com/2015/03/10/politics/state-department-hack-worst-ever/, last visited: 6 May 2016.

[22] Schmidt, M. S. and David E. Sanger, 'Russian Hackers Read Obama's Unclassified Emails, Officials Say', *The New York Times*, 25 April 2015, available at: http://www.nytimes.com/2015/04/26/us/russian-hackers-read-obamas-unclassified-emails-officials-say.html, last visited: 6 May 2016.

[23] Perez, E. and Shimon Prokipecz, 'How the U.S. thinks Russians hacked the White House', CNN, 8 April 2015, available at: http://edition.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/, last visited: 13 May 2016.

[24] Hacquebord, F. 'Pawn Storm Targets MH17 Investigation Team', *Trend Micro*, 22 October 2015, available at: http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-targets-mh17-investigation-team/, last visited: 6 May 2016.

been released. In it, fake servers of the Board were created in order to carry out credential phishing attacks.[25] The aim was to gain access to the Board's real servers, and thereby gain unauthorised access to sensitive material collected by Dutch, Malaysian, Australian, Belgian, and Ukrainian authorities.

Those responsible for the attack, according to experts, were likely to be Pawn Storm, otherwise known as Advanced Persistent Threat 28 (APT28). APT28 is believed to be based in Russia and to have close links to the Russian government. According to the cybersecurity firm *FireEye*, the group has a history of targeting "insider information related to governments, militaries, and security organizations that would likely benefit the Russian government".[26]

## *4.3 Think Tanks and Policy Communities*

In April 2009, a US-based foreign policy think tank was hit by cyberattacks. Over the course of two days, between 16 and 17 April, various personnel received emails containing attachments of malicious Microsoft Word documents and PDF files, in an attempt to infiltrate the organisation. Over the same two-day period, on the other side of the Atlantic, government institutions in both Czech Republic and Poland were subjected to the same treatment. The attacks began only days after President Barack Obama gave a major foreign-policy speech, on 5 April, in which he declared his intention to proceed with the deployment of the US's "European Interceptor Site" missile defence base in Poland, with a related radar station located in the Czech Republic.[27]

According to F-Secure Labs, the Finnish cybersecurity firm, the attacks were carried out by "The Dukes" – "a well-resourced, highly dedicated and organized cyberespionage group that ... has been working for the Russian Federation since at least 2008 to collect intelligence in support of foreign and security policy decision-making".[28]

## *4.4 Media and Press*

In April 2015, TV5Monde, a major French television network, was attacked by cybercriminals. In the attack, hackers gained control over the network's ten news channels and its social media channels and published jihadist propaganda, including publish personal information of French soldiers serving in Syria. After an initial blackout, the station resumed broadcasting within hours and later regained control of its Facebook and Twitter pages. The hackers initially claimed to be ISIS militants, part of the so-called "CyberCaliphate", but it soon became apparent that they were, in fact, members of the Russian group APT28.[29] The attack had been well planned, beginning three months earlier, in January, when hackers sent phishing emails to journalists at the network.

[25] This is when emails are sent from what appears to be a trusted source in order to trick the recipient into opening a malicious attachment or visiting a malicious website where malware is downloaded to their computer.

[26] 'APT28: A Window Into Russia's Cyber Espionage Operations?', *FireEye*, 5 February 2010, available at: https://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf, last visited: 6 May 2016, p. 4.

[27] 'The Dukes: 7 years of Russian cyberespionage', F-Secure Labs Threat Intelligence Whitepaper, 29 January 2011, available at: https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf, last visited: 6 May 2016, p. 5.

[28] Ibid., p. 3.

[29] Riley, M. and Jordan Robertson, 'Cyberspace Becomes Second Front in Russia's Clash With NATO', *Bloomberg*, 14 October 2015, available at: http://www.bloomberg.com/news/articles/2015-10-14/cyberspace-becomes-second-front-in-russia-s-clash-with-nato, last visited: 6 May 2016.

It is not just the broadcast media that APT28 have targeted, either. Print media have also fallen victim to cyberattacks. In December 2014, a prominent military correspondent for a large US newspaper suffered a cyberattack on his personal email address, which likely leaked his credentials. Later the same month, [30] APT28 attacked around 55 employees of the same newspaper on their work email accounts.

A year earlier, in late 2013, a journalist received an email from the Chief Coordinator of US-based *Reason* Magazine's Caucasian Issues Department. The email welcomed him as a contributor and requested topic ideas and identification information in order to establish him at the magazine. This ought to have piqued the journalist's interest, as the magazine does not have such a department. Nevertheless, the journalist opened one of the files attached to the email and, unbeknown to him, unleashed malware on to his computer. The malware, it was later established, had been created by APT28.[31]

## *4.5 Industry*

In 2014, an unnamed steel mill somewhere in Germany was hit by cyberattacks, with massive real-life (or, to use the technical term, "cyber-to-physical") effects. It is not clear when the attack in Germany took place, but it came to light in Germany's annual IT Security report, released just before Christmas.[32] The report, issued by Germany's Federal Office for Information Security, said that hackers had gained access to the steel mill through the plant's business network, and then worked their way through various networks to access systems controlling plant equipment. They had such control that a blast furnace could not be properly shut down, resulting in "massive" – though unspecified – damage.[33]

The hackers infiltrated the corporate network using a spear-phishing attack. Once they had a foothold on one system, they were able to explore the company's networks and eventually compromise a "multitude" of systems, including industrial components on the production network. Digital traces left in the system point to Russian involvement, but not conclusively to the government itself, according to a US intelligence assessment.[34]

## *4.6 Energy*

In late 2015, two of Ukraine's energy companies – one in Ivano-Frankivsk Oblast and the other in Kyiv Oblast – were hit by cyberattacks, leaving some 80,000 homes without power. Hackers had entered the two companies' management systems, possibly through a spear-phishing campaign, and disconnected breakers at their energy substations. At roughly the same time, the companies' telephone call centres were hit by a DDoS attack. The hackers then paralysed the entire companies' systems, and malware affected computers and servers. In most cases, power was restored within three hours, but because the hackers had sabotaged the companies' management systems,

[30] Hacquebord, F. 'Operation Pawn Storm Ramps Up its Activities; Targets NATO, White House', TrendMicro, 16 April 2015, available at: http://blog.trendmicro.com/trendlabs-security-intelligence/operation-pawn-storm-ramps-up-its-activities-targets-nato-white-house/, last visited: 13 May 2016.
[31] The Dukes: 7 years of Russian cyberespionage", F-Secure Labs Threat Intelligence Whitepaper, 29 January 2011, pp. 10-11.
[32] 'Die Lage der IT-Sicherheit in Deutschland 2014', Bundesamt für Sicherheit in der Informationstechnik, 15 December 2014, available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile, last visited: 6 May 2016.
[33] Zetter, K. 'A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever', *Wired*, 1 August 2015, available at: http://www.wired.com/2015/01/german-steel-mill-hack-destruction/, last visited: 6 May 2016.
[34] Riley, M. and Jordan Robertson, 'Cyberspace Becomes Second Front in Russia's Clash With NATO', Bloomberg, 14 October 2015.

technicians had to physically travel to substations to manually close breakers that the hackers had digitally opened.[35]

The attacks featured a modified version of the Russia-designed "BlackEnergy", which is a kind of malware known as a Trojan horse that remotely takes over computers in order to carry out DDoS attacks.[36] The US-based security firm iSight Partners associates this particular malware with a cybercriminal group it calls the Sandworm Team, which it believes is tied to the Russian government.[37]

In August of the previous year, Norway's National Security Authority (NSM) announced that cyberattacks had compromised as many as 50 Norwegian oil companies, including Statoil, its largest, state-owned oil firm. The NSM advised 250 other energy companies to check their networks for evidence of malicious activity. Several reported that their networks had been compromised. In one case, cybercriminals had sent a phishing email with a malicious attachment to a high-ranking employee in the procurement division at a Nordic energy company. The email purported to be from the company's human resources team and threatened the employee with dismissal. Cybercriminals also sent phishing emails, again appearing to be from human resources' representatives, to several other company employees.

This activity is associated with the suspected Russian actors behind the Fertger/Havex malware family, which other researchers refer to as "Energetic Bear" or "Dragonfly".[38]

## *4.7 Finance*

In mid-August 2014, JPMorgan Chase & Co. and at least one other US bank were hit by cyberattacks. In one case, hackers used a software flaw known as a zero-day vulnerability (which is to say, a vulnerability in software that hackers can exploit and for which the creator of the software has zero-days in which to mitigation its exploitation) in one of the banks' websites. They then ploughed through layers of elaborate security to steal gigabytes of sensitive data. As many as 76 million households and 7 million small business may have had data compromised.[39]

The attack followed a recent infiltrations of major European banks using a similar vulnerability, and nine other US and international financial institutions – including, Bank of America, Regions Bank, TD Bank, and Commercial Bank International of UAE – were also targeted.[40]

[35] Zetter, K. 'Everything We Know About Ukraine's Power Plant Hack', *Wired,* 20 January 2016, available at: https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/, last visited: 6 May 2016.
[36] See: Kovacs, E. 'Ukraine Accuses Russia of Hacking Power Companies', *Security Week*, 30 December 2015, available at: http://www.securityweek.com/ukraine-accuses-russia-hacking-power-companies, last visited: 6 May 2016.
[37] Hultquist, J., 'Sandworm Team and the Ukrainian Power Authority Attacks', *iSight,* 7 January 2016, available at: https://www.isightpartners.com/2016/01/ukraine-and-sandworm-team/, last visited: 6 May 2016.
[38] 'Cyber Threats to the Nordic Region', *FireEye*, 11 May 2015, available at: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-nordic-threat-landscape.pdf, last visited: 6 May 2016, p. 10.
[39] Goldstein, M. and Perlroth, N. and David E. Sanger, 'Hackers' Attack Cracked 10 Financial Firms in Major Assault', The New York Times, 3 October 2014, available at: http://dealbook.nytimes.com/2014/10/03/hackers-attack-cracked-10-banks-in-major-assault/?_php=true&_type=blogs&_r=1 last visited: 13 May 2016.
[40] Waterman, S. 'US banks targeted in new Russian hack', Politico, 5 December 2015, available at: http://www.politico.eu/article/us-banks-russia-hack-malware-cyber/, last visited: 13 May 2016.

The FBI initially linked the hackers to Russia, and cybersecurity experts have added further substance to this belief since. The US-based cybersecurity firm root9B analysed the malware used in the hacks and found code and signatures previously associated with APY28.[41]

Eleven months earlier, on 23 October 2013, the Warsaw Stock Exchange was hit by a series of cyberattacks. Data were stolen, client login details were made public online, and the Exchange's systems were made accessible to cybercriminals of all stripes. It was sabotage by crowd-sourcing. The hackers claimed to be from ISIS, but were in fact Russian, members of APT28.[42]

## 5. The Kremlin's Fingerprint?

Vladimir Putin may have disparagingly characterised the Internet as a "CIA invention", but he is determined to control it.

Since he returned to the presidency in 2012, Putin has poured significant money and manpower into this endeavour. In 2015, he ordered the FSB, Russia's Federal Security Service, to "cleanse the Russian Internet" by forcing all Internet providers to keep their servers in Russia.[43] During the Sochi Olympics in February 2014, the FSB deployed aggressive cyber-spying tools designed to infect foreign visitors' computers and mobile phones with spyware through Wi-Fi networks and mobile phone towers.[44] In 2012, meanwhile, Putin pledged to create a separate Russian Internet, and has put some US$100 million towards it.

While Putin has busied himself trying to master the Internet, there is uncertainty over who exactly is behind the cyberattacks from which Russia so evidently benefits. As with its more conventional warfare, Russia has intentionally blurred the dividing line between state and non-state.

As well as having its own cyber specialists, the FSB reportedly recruits hackers to launch cyberattacks when it wants to punish or silence the Kremlin's rivals. For at least the last decade, the Kremlin has sourced technology and even intelligence information from cyber-crime groups within its near abroad – the so-called "Silicon Valley of Eastern Europe".[45] The result of this, according to cyber-threat analyst Jonathan Wrolstad, is that Russia possesses some of the most sophisticated hacking teams in the world. Russian hacking groups, says Wrolstad, write the "best pieces of malware", some of which are "almost impossible for an organization to detect".[46]

Dmitri Alperovitch, co-founder of the security firm CrowdStrike, which monitors Russian cybercrime, has observed one of the tactics used by the Russian security services to recruit hackers. In an interview with *The Hill*, Alperovitch explained: "When someone is identified as being

[41] 'APT28 Targets Financial Markets: Zero Day Hashes Released', root9B, 5 November 2015, available at: http://www.mediafire.com/download/bdr77piwp0ij0qz/FSOFACY.pdf, last visited: 13 May 2016.
[42] Riley, M. and Jordan Robertson, 'Cyberspace Becomes Second Front in Russia's Clash With NATO', *Bloomberg*, 14 October 2015.
[43] 'Russia Update: At FSB Meeting, Putin Portrays Russia as Innocent Victim of Hostile World', *The Interpreter*, 26 March 2015, available at: http://www.interpretermag.com/russia-update-march-26-2015/, last visited: 6 May 2016.
[44] Matthews, O., 'Russia's Greatest Weapon May Be Its Hackers', *Newsweek*, 5 July 2015, available at: http://www.newsweek.com/2015/05/15/russias-greatest-weapon-may-be-its-hackers-328864.html, last visited: 6 May 2016.
[45] One reason for the prevalence of such individuals is the Soviet legacy of emphasising maths and science education, which has resulted in high-qualified software writers and hackers. See, Flook, K. 'Russia and the Cyber Threat', *Critical Threats*, 13 May 2009, available at: http://www.criticalthreats.org/russia/russia-and-cyber-threat, last visited: 11 May 2016.
[46] Bennett, C., 'Kremlin's ties to Russian cyber gangs sow US concerns', *The Hill*, 11 October 2015, available at: http://thehill.com/policy/cybersecurity/256573-kremlins-ties-russian-cyber-gangs-sow-us-concerns, last visited: 6 May 2016.

technically proficient in the Russian underground," a criminal case is brought against them and then they suddenly disappear "and those people are never heard from again". Alperovitch adds that the hacker in question is then working for the Russian security services.[47]

Such a strategy – of offering a hacker convicted of cybercrimes the opportunity to work for the FSB instead of receiving a prison sentence – is not new. Oleg Gordievsky, the KGB colonel who defected to MI6 in 1985, described this as early as 1998.[48]

It is unclear, however, precisely how much direction cybercriminals are given by the Kremlin. As with its more conventional warfare, Russia has intentionally blurred the dividing line between state and non-state, war and peace. Hackers are often suspected of having close ties to the Kremlin and acting with its approval, but the exact nature of the link remains murky.

Nevertheless, it is possible to identify links. Beyond the digital signatures they create, the language in which they write, and the times of day when they are active, a key indicator of hackers' allegiances are the individuals or entities they target.

Take APT28, for example. The language much of the code the group write in is Russian, and it is written at times of the day that correspond to business hours in the UTC + 4 time zone, which includes Moscow and St. Petersburg. According to *FireEye,* the US cyber security firm that has tracked the group over a number of years:

> many of APT28's targets align generally with interests that are typical of any government. However, three themes in APT28's targeting clearly reflects areas of specific interest to an Eastern European government, most likely the Russian government. These include the Caucasus (especially the Georgian government), Eastern European governments and militaries, and specific security organizations.[49]

Or consider "The Dukes". The group, says *F-Secure Labs*, has engaged in "biannual large-scale spear-phishing campaigns against hundreds or even thousands of recipients associated with governmental institutions and affiliated organizations", and it notes that "the targets and timing of these campaigns appear to align with the known foreign and security policy interests of the Russian Federation at those times".[50]

Cyberwarfare is one of a number of areas in which the Kremlin demonstrates behaviour that is more common among criminal syndicates than permanent members of the United Nations Security Council. The distinction between honest government and criminal graft, however, may be an unhelpful one. Jose Grinda, a Spanish prosecutor, spent more than a decade investigating the spread of Russian organised crime during the Putin era and came to the conclusion, published in

[47] Bennett, C., 'Kremlin's ties to Russian cyber gangs sow US concerns', *The Hill*, 11 October 2015, available at: http://thehill.com/policy/cybersecurity/256573-kremlins-ties-russian-cyber-gangs-sow-us-concerns, last visited: 6 May 2016.
[48] Flook, K. 'Russia and the Cyber Threat', *Critical Threats*, 13 May 2009, available at: http://www.criticalthreats.org/russia/russia-and-cyber-threat, last visited: 11 May 2016.
[49] 'APT28: A Window Into Russia's Cyber Espionage Operations?', *FireEye*, 5 February 2010, available at: https://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf, last visited: 6 May 2016, p. 6
[50] Ibid., p. 3.

2015 as a 488-page complaint, that the activities of Russian criminal networks are virtually indistinguishable from those of the government.[51]

# 6. What Is Being Done?

In April 2015, 400 soldiers and civilians gathered in a hotel in the Estonian capital Tallinn to take part in NATO's biggest ever cyberwar game. The location of the exercise could hardly have been more symbolic. Estonia had learned the importance of cyber defence the hard way. Russia's cyberattacks on Estonia, in 2007, were not only an early display of the vulnerability of modern societies to this new form of aggression but also an example of what has now become known as hybrid warfare.

In anticipation of the next big attack, NATO established the Cooperative Cyber Defence Centre of Excellence in Tallinn. Estonia had initially proposed the concept to NATO in 2004, right after joining the Alliance, but it took four years before it was created, in May 2008.[52] .[53] The Centre's establishment followed NATO's inclusion of cyberattacks as one of the key issues facing the Alliance, in 2010's "Strategic Concept".[54]

NATO's proactivity has been mirrored by its member states, including the UK.

In March 2016, the UK government announced that a National Cyber Security Centre, led by GCHQ, would be set up in London.[55] The Centre's creation had first been muted in November 2015 when, in wake of criticisms that the UK's cyber defences were inadequate, Chancellor George Osborne announced that the government would establish a cybersecurity centre and spend £2 billion on cyber defences. A year earlier, the UK established a Computer Emergency Response Team; an organisation that will coordinate the management of cyber incidents and act as the central contact point for international counterparts. This followed on from the adoption, in November 2011, of "The UK Cyber Security Strategy".[56]

It is not only in the cyber realm that the UK has been active, either. In April 2015, the British Army created a new unit, the 77th Brigade, skilled in psychological operations and use of social media to engage in unconventional warfare.[57] Earlier still, in 2013, the Joint Cyber Reserve unit was established, which is intended to recruit hundreds of hackers as reservists.[58] The collective aim is to sharpen the British military's ability to bolster its defences. The Reserve unit also carries out cyberattacks, signifying the government's willingness to strike against intruders or even take pre-emptive action.

[51] Duarte, E. and Henry Meyer, 'Putin Allies Aided Russian Mafia in Spain, Prosecutors Say', *Bloomberg*, 29 June 2015, available at: http://www.bloomberg.com/news/articles/2015-06-29/putin-allies-aided-russian-mafia-in-spain-prosecutors-say, last visited: 6 May 2016.

[52] 'NATO opens new centre of excellence on cyber defence', NATO, 14 May 2008, available at: http://www.nato.int/docu/update/2008/05-may/e0514a.html, last visited: 6 May 2016.

[53] Ibid.

[54] 'Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation', NATO, 20 November 2010, available at: http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf, last visited: 9 May 2016.

[55] 'Press release: New National Cyber Security Centre set to bring UK expertise together', GCHQ, 18 March 2016, available at: https://www.gov.uk/government/news/new-national-cyber-security-centre-set-to-bring-uk-expertise-together, last visited: 6 May 2016.

[56] 'The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world", UK Government, 25 November 2011, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf, last visited: 9 May 2016.

[57] MacAskill, E. 'British army creates team of Facebook warriors', *The Guardian*, 31 January 2015, available at: http://www.theguardian.com/uk-news/2015/jan/31/british-army-facebook-warriors-77th-brigade, last visited: 9 May 2016.

[58] Borger, J. '"Trident is old technology": the brave new world of cyber warfare', *The Guardian*, 16 January 2016.

Taken together, these developments suggest that the West – and the UK in particular – is moving in the right direction in combatting the threat posed by Russia's cyberwarfare. Nevertheless, more could be done.

# 7. Conclusions and Policy Recommendations

Russia is not alone in using cyberwarfare against the West. In China in 2013, the now infamous Unit 61398 of the People's Liberation Army – more formally known as the General Staff Department, Third Department, Second Bureau – was discovered to have been running an almost constant cyber-offensive against Western companies and governments for seven years, from a 12-storey building in Shanghai.[59] Hackers in North Korea, meanwhile, were responsible for an attack on Sony Pictures in late 2014, in which its systems were crippled and terabytes of data were leaked online.

Russia poses a specific threat, however, as it is the only country to date to have combined cyberwarfare with conventional warfare. And it has done so twice in the last decade – in Georgia in 2008, and in Ukraine since 2014 – with some success. Given recent events in Eastern Europe and Middle East, there can be little question about the aggressiveness of Russia's foreign policy. And cyberwarfare is increasingly playing a greater role in this. Faced with such a situation, the West needs to develop more effective ways to deal with Russia's cyberwarfare.[60] In an ideal world, these would be tools that reduce the threat facing Western capitals and maximise the cost to Moscow.

There are a number of policy recommendations that arise from the findings of this paper:

- **Zero tolerance for cyberattacks.** Deterrence in cyberwarfare is more uncertain than, say, in nuclear strategy. There is no 'mutually-assured destruction', the dividing line between peace and war is blurred, and identifying those conducting the war, let alone whom they report to, is difficult. Nevertheless, where there is evidence that individuals or countries are behind cyberattacks, they should feel the full force of the law. After the Kremlin-orchestrated murder of Alexander Litvinenko, Britain expelled Russian diplomats, limited visas for Russian officials, and stopped intelligence sharing and police cooperation. After Russia hacked US banks in 2014, Washington did nothing but call for investigations and encourage financial institutions to take cybersecurity more seriously.[61] If there were zero tolerance for Russia's cyberattacks, this would not only send a political message – the Kremlin currently sees the West as being rather 'soft' – but would also deliver a blow to these activities.

- **Adopt an integrated approach to cybersecurity.** While the concept of cyberwarfare appears to be well understood by Western governments, the various aspects of what constitutes 'cyberwarfare' are not being address together. In the US, for example, the head of country's

[59] Jourdan, A., 'China-U.S. cyber spying row turns spotlight back on shadowy Unit 61398', *Reuters*, 20 May 2014, available at: http://www.reuters.com/article/us-cybercrime-usa-china-unit-idUSBREA4J08M20140520, last visited: 6 May 2016.

[60] Galeotti, M., 'Who Needs Assassins When You've Got Hackers?', *The New York Times*, 22 January 2016, available at: http://www.nytimes.com/2016/01/23/opinion/who-needs-assassins-when-youve-got-hackers.html, last visited: 6 May 2016.

[61] Riley, M. and Jordan Robertson, 'FBI Said to Examine Whether Russia Tied to JPMorgan Hacking', *Bloomberg*, 27 August 2014, available at: http://www.bloomberg.com/news/articles/2014-08-27/fbi-said-to-be-probing-whether-russia-tied-to-jpmorgan-hacking, last visited: 6 May 2016.

Cyber Command Admiral Michael S. Rogers released a statement, in September 2015, describing how it would defend the US Department of Defence against cyberattacks and provide support to military and contingency operations.[62] This approach is more integrated than in other Western countries, but this is only the case within the military. Such compartmentalised thinking could lead to gaps in security, not least with regards civilian infrastructure.

- **Increase funding for cybersecurity education programmes.** Cybersecurity is not primarily a cyber issue. As Edward Lucas has argued, "All the locksmiths in the world won't protect people who care carless with their keys."[63] Estimates suggest that around nine-tenths of the 140 billion emails sent daily are spam, of which around one-sixth are 'phishing' scams. Such attacks are a major issue if the attacker gains access to classified information, but even a breach of unclassified email systems poses major security risks. This is because all sorts of sensitive information is routinely shared in non-classified emails. In a number of the cases detailed in this report, Russia's cyberattacks succeeded because individuals fell for such scams. Thus, widespread cybersecurity education programmes are needed.

- **Prepare for scenarios in which access to the Internet is limited.** Cyber technology is everywhere, in civilian and military life. Growing connectivity over networks, however, leaves open the possibility that access to those networks may be limited or impaired. Take undersea fibre-optic cables, for example. More than nine-tenths of internet traffic travels through such cables, and these are dangerously bunched up in a few key points – around New York, near the Red Sea and Gulf of Aden, and at the Luzon Strait in the Philippines. Such bunching makes the cables, together with their termination points and exchange points, an obvious target for both hackers and terrorists. This suggest two things. First, civil and military contingency planning should include scenarios in which access to the Internet is limited. Second, internet infrastructure – including satellites and their bases stations, – needs at least as much defence and protection as other strategic assets.

[62] Garamone, J. 'U.S. Cyber Command Chief Details Plans to Meet Cyberspace Threats',
US Department of Defense, 8 September 2015, available at: http://www.defense.gov/News-Article-View/Article/616512/us-cyber-command-chief-details-plans-to-meet-cyberspace-threats, last visited: 9 May 2016.

[63] Lucas, E. 'We make life too easy for online fraudsters', *The Times*, 7 May 2016, available at: http://www.thetimes.co.uk/article/we-make-life-too-easy-for-online-fraudsters-2bggf9rxw?acs_cjd=true, last visited: 9 May 2016.

## About the Author

**Dr Andrew Foxall** is Director of the Russia Studies Centre at The Henry Jackson Society. His first book, *Ethnic Relations in Post-Soviet Russia*, was published by *Routledge* in October 2014. Andrew holds a DPhil from the University of Oxford.

## Acknowledgements

I should like to thank Simas Celutka for his ideas and assistance.

## About the Russia Studies Centre

The Russia Studies Centre is a research and advocacy unit, operating within The Henry Jackson Society, dedicated to analysing contemporary political developments and promoting human rights and political liberty in the Russian Federation.

## About The Henry Jackson Society

The Henry Jackson Society is a think-tank and policy-shaping force that fights for the principles and alliances which keep societies free, working across borders and party lines to combat extremism, advance democracy and real human rights, and make a stand in an increasingly uncertain world.

RUSSIA STUDIES CENTRE
AT THE HENRY JACKSON SOCIETY

The Henry Jackson Society
Millbank Tower,
21-24 Millbank, London, SW1P 4QP
Tel: 020 7340 4520

**www.henryjacksonsociety.org**
Charity Registration No. 1140489

The views expressed in this publication are those of the author and are not necessarily indicative of those of The Henry Jackson Society or its Trustees

THE HENRY JACKSON SOCIETY
DEMOCRACY·FREEDOM·HUMAN RIGHTS