THE CYBER-ENABLED INFORMATION STRUGGLE 220

RUSSIA'S APPROACH AND WESTERN VULNERABILITIES

Veli-Pekka Kivimäki

FIIA BRIEFING PAPER 220 ▪ May 2017

ULKOPOLIITTINEN INSTITUUTTI
UTRIKESPOLITISKA INSTITUTET
THE FINNISH INSTITUTE OF INTERNATIONAL AFFAIRS

THE CYBER-ENABLED INFORMATION STRUGGLE

RUSSIA'S APPROACH AND WESTERN VULNERABILITIES

Veli-Pekka Kivimäki
Researcher
Finnish Defence Research Agency

FIIA Briefing Paper 220
May 2017

- Cyber operations related to recent elections are symptomatic of the ongoing 'information struggle' with the West that Russia sees itself as being engaged in.
- To the Russian way of thinking, the information space ties the technical and psychological domains together, both of which are utilized to achieve the desired effects. Cyberspace is not restricted to the technical domain, but can also be used to achieve effects in the psychological domain.
- Individuals are currently insufficiently protected against nation-state actors in cyberspace, creating vulnerabilities in democratic societies. Governments need to find ways to counter and deter attacks against their citizens in cyberspace as well.
- Attributing cyber attacks is an effort in interpreting the technical breadcrumb trail left behind after attacks, but when dealing with nation-state actors, the political cost of attribution becomes a factor in determining responses.

ULKOPOLIITTINEN INSTITUUTTI
UTRIKESPOLITISKA INSTITUTET
THE FINNISH INSTITUTE OF INTERNATIONAL AFFAIRS

Introduction

As our digital habitat, cyberspace is home to services that connect people across national borders, and increasingly through social media. With over 80% of the population in the US and Europe online, for the most part through mobile devices, social media is extending its reach and increasingly being used for real-time communications. Content knows no boundaries, and information from across the globe can be accessed at the push of a button. As such, cyberspace also offers a conduit for misinformation, which can be driven by dubious commercial motives, as well as by national actors wishing to advance their objectives. Hence, cyberspace can be viewed as an operating environment in its own right, but also as a vector for achieving effects more broadly in the information environment, and for influencing public sentiments.

The United States presidential campaign of 2016 brought the issue of state-sponsored cyber attacks to the fore in the public discourse, particularly after the assessment conducted by the US Intelligence Community, which linked Russia to the hacking of the Democratic National Committee (DNC) and the subsequent leaks of Hillary Clinton's campaign emails. Meanwhile in Europe, the French foreign minister condemned alleged Russian cyber attacks on the French election campaigns. These types of attacks are symptomatic of a broader pattern in which the democratic principles of Western societies are being turned into vulnerabilities.[1]

Influence operations through social media can feed into societal fault lines, reinforcing fragmentation and the formation of information bubbles. This effect was illustrated in a study on the dissemination of false information in social media during the 2016 US elections, which found that users in ideologically segregated groups are more likely to believe ideologically aligned headlines, whether true or false.[2] This taps directly into the psychological effect known as confirmation bias, whereby recipients of information who already hold a strong view on a subject are more likely accept new information fitting this pre-determined position, without critically evaluating the new input. Thus, in the case of fabricated 'news', these information bubbles provide fertile ground for its propagation. The inherent danger in this effect is that it can be weaponized for information operations, for example by fomenting violent nationalistic sentiments.

Western thinking and doctrine on cyberspace operations often emphasize the technological aspects of the operations. However, in assessing the Russian operations, it is beneficial to understand the activities in the context of Russian thinking on the information space and to what ends it might be utilized. This paper also examines some challenges for the West, namely how to protect individuals from nation-state actors in cyberspace, and how the dynamics of attack attribution can complicate responses by governments.

Russia's approach to the information struggle

Russian military thinking views the information space holistically, recognizing the importance of psychological effects.[3] In contrast with the Western concept of cyber operations, Russian writing refers to information-technical effects as a subcomponent of the overarching information struggle, *informatsionnoye protivoborstvo*. The word "struggle" aptly describes the Russian approach, as the term "information warfare" conveys a mental image of an overt and clearly identifiable conflict, while in reality the actions are thought to be ongoing even in peacetime.[4] This also contributes to ambiguity,

1 B. Renz & H. Smith (eds.), 'Russia and Hybrid Warfare: Going Beyond the Label', *Aleksanteri Institute, University of Helsinki*, Aleksanteri Papers 1/2016, 22 April 2016, p. 57.

2 H. Allcott & M. Gentzkow, 'Social Media and Fake News in the 2016 Election', Journal of Economic Perspectives (forthcoming), 31 March, 2017, https://web.stanford.edu/~gentzkow/research/fakenews.pdf, accessed 12 April 2017.

3 D. Adamsky, 'Cross-Domain Coercion: The Current Art of Russian Strategy', *Proliferation Papers*, No. 54, November 2015, p. 29.

4 R. Heickerö, 'Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations', Swedish Defence Research Agency (FOI), 2010, pp. 18–20.

which may be a desirable feature of influence operations – does the target even realize that they are the subject of such actions?

In 2013 Russian military thinkers provided insights into how the Russian military leadership characterized the nature of future wars, and the role of psychological operations therein. The now famous article by Chief of the General Staff Valery Gerasimov[5] on what some interpret as a recipe for "hybrid warfare", as well as an article in the Russian Ministry of Defence's journal *Military Thought*[6], elaborate on what new-generation warfare might look like. Specifically, aggressors are expected to use non-military actions, utilizing "powerful information technologies", and involving all the public institutions of the target country, with the goal of undermining the target's social system. This is in line with interpretations published as a part of Jānis Bērziņš's 2014 report on Russian new-generation warfare, whereby the human mind is seen as the primary battlefield, with information and psychological warfare playing a dominant role.

Russia's information security doctrine of 2016 reflects this view from the perspective of protecting national interests in cyberspace, to the extent that the free flow of information could be restricted by technical means as needed. In the longer term, this is indicative of a possible desire to further segregate the Russian part of the Internet, also known as Runet, from the greater Internet. The degree to which complete separation is possible is contentious, but Russian efforts in this regard warrant monitoring. Restricting access to international information sources would make any comparative assessment of world affairs more difficult for Russia's citizens.

As the Soviet-era concept of reflexive control has resurfaced in recent times as Western analysts seek to understand Russia's influence operations, the concept of political warfare may warrant consideration while endeavouring to understand the big picture when it comes to Russia's actions. In 1989, former CIA officer Donald Jameson, who was responsible for defectors and Soviet covert operations, wrote about the Soviet approach to political warfare, stating that foreign policy manipulation was a survival tool for the Soviet Union.[7] Considering recent Russian interference in the elections in the US and Europe, it is worth considering how representative this might be of current foreign policy logic, and whether foreign policy manipulation is still considered a tool for internal stabilization.

Individuals as targets

Since the information struggle is an ongoing activity during peacetime as well, individuals are already finding themselves caught up in it. Indeed, a troubling emerging trend is the targeting of individuals by state-affiliated cyber-enabled campaigns. In a 2016 assessment of the future military operating environment up to 2035, the United States Joint Chiefs of Staff predicted that influence operations would have an increasing focus on individual citizens and decision-makers. Cyberspace is a key factor in enabling this reach. The digital transformation of society means that more and more data is generated on each individual in both public and private sector databases. Such data could also be a coveted target for intelligence and offensive purposes.

Individuals can be an important vector for gaining covert access to information systems. A typical, not very sophisticated but highly effective method is 'spear phishing', whereby the targeted individual is deceived into either executing malicious software or surrendering their user credentials. While the risks emerging from these types of attacks can be managed in government-controlled networks through various technical means, the targeting of private persons online is a greater challenge to manage. This leaves political field organizations, for example, vulnerable to attack, a risk highlighted by the DNC hack.

In addition to governmental and political targets, civil activists and journalists are increasingly being targeted by actions through cyberspace. During the past few years, there has been a marked uptick

5 V. Gerasimov, 'The Value of Science is in the Foresight', *Military-Industrial Kurier*, 27 February, 2013 (Translated by R. Coalson).

6 S. G. Chekinov & S. A. Bogdanov, 'The Nature and Content of a New-Generation War', *Military Thought*, No. 4, 2013.

7 D. Jameson, 'Comment', in C. Lord & F. R. Barnett (eds.), *Political Warfare and Psychological Operations*, National Defense University Press, 1989, p. 104.

in attempted attacks targeting journalists, mostly made visible by service providers such as Google, which have started notifying their users about potential state-sponsored attacks. Individuals engaged in independent research on the Ukraine conflict have also been targeted by attacks linked to state-sponsored actors, including this author. Further, in its 2017 annual report, the Norwegian Police Security Service noted that individuals are increasingly being targeted by the Russian intelligence services. This poses new dilemmas about the role of governments in protecting their citizens against cyber attacks.

Online attacks against individuals take a particularly disturbing form when they are coercive in nature, such as persistent personal attacks and the dissemination of false information. This type of online activity is sometimes dismissed as 'trolling', taking its name from internet parlance and referring to provocative and offensive commentary, but this risks diluting the seriousness of such attacks.

The current targeted attack campaigns against journalists, for example, are a troubling indicator of behaviour that can be weaponized in an attempt to limit free speech or to silence political opponents. The targeted psychological subversion of opponents is nothing new, and was previously institutionalized by East Germany's Stasi as *Zersetzung*,[8] utilized in operations against dissidents in order to break their will to resist. Activities resembling this method are now being engaged in through cyberspace.[9] If such campaigns were organized by state-sponsored actors, the results could be highly disruptive and severely impede the civil liberties of individuals.

While governments provide protection for their citizens in the physical realm, in the form of armed forces providing military protection against threats to society, and police forces protecting individuals against violence in their daily life, the government's role and means of protecting the basic human rights of their citizens in the digital realm is less clear. This concern has now been raised by the technology industry as well, with Microsoft's chief legal officer calling for a Digital Geneva Convention to protect civilians against nation-state attacks.[10]

Complicating the issue is the perception of governments intruding into people's digital lives. Particularly following the revelations of Edward Snowden, even targeted network monitoring efforts are erroneously labelled as "government mass surveillance". The flipside of the issue is that carefully scoped monitoring efforts, with proper judicial oversight, could actually reveal traces of cyber attacks against individuals, too. If the government has no means to detect attacks, the burden of detection will be left to organizations and individuals.

The politics of attribution

When it comes to governments responding to offensive cyber or influence operations, whether targeting organizations or individuals, the correct attribution of the attack to the responsible party becomes a central issue. In order to hinder attribution, front organizations have been created in an attempt to complicate matters, and shield the responsible state-affiliated actors. In the case of the US election hacking incident, front organizations and personas such as 'Guccifier 2.0' have formally accepted responsibility for perpetrating detected attacks, while leak-anonymizing organizations like WikiLeaks have been used as outlets for distributing information acquired during an intrusion.[11] Regardless of obfuscation attempts, a joint release by the Department of Homeland Security and the Federal Bureau of Investigation connected the cyber

8 Ministerium für Staatssicherheit, 'Richtlinie Nr. 1/76 zur Entwicklung und Bearbeitung Operativer Vorgänge (OV)', *Stasi Records Agency (BStU)*, January 1976, http://www.bstu.bund.de/DE/Wissen/MfS-Dokumente/Downloads/Grundsatzdokumente/richtlinie-1-76_ov.html, accessed 13 February, 2017.

9 E.g. A. Higgings, 'Effort to Expose Russia's Troll Army Draws Vicious Retaliation', *The New York Times*, 30 May 2016, https://www.nytimes.com/2016/05/31/world/europe/russia-finland-nato-trolls.html, accessed 13 February, 2017.

10 B. Smith, 'The need for a Digital Geneva Convention', *Microsoft On the Issues*, 14 February, 2017, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/, accessed 7 May, 2017.

11 T. Rid, 'Disinformation: A Primer in Russian Active Measures and Influence Campaigns', *Select Committee on Intelligence, U.S. Senate*, 30 March, 2017, https://www.intelligence.senate.gov/sites/default/files/documents/os-trid-033017.pdf, accessed 12 April, 2017.

campaign targeting the DNC to the Russian intelligence services, and duly dubbed the campaign *Grizzly Steppe*.

In attributing attacks, cyber security expert Dmitri Alperovitch has noted[12] that the attribution of cyber attacks has been carried out for several decades, but that the issue became controversial only when it assumed a political dimension. Attributing attacks to criminal organizations has been widely accepted, but once inter-state relations are at stake, the dynamics of assigning the blame may change. Thomas Rid and Ben Buchanan make the same point in their 2013 article, stating that at a strategic level "attribution is a function of what is at stake politically".[13] At a technical level, attributing an attack calls for a forensic investigation of the digital evidence left behind after an attack, but how that evidence is interpreted may be affected by what the political cost of the attribution amounts to.

This difference in the attribution calculus can clearly be seen in the stances taken by the Obama and Trump administrations towards the DNC hack and email leak. The attribution of the DNC breach to Russia was made by the US Intelligence Community in a declassified version of a report on the incident. The DNC hack and email release was labelled as election interference, and was one of the reasons for the additional sanctions imposed on the Russian intelligence services in late December 2016, in addition to the expulsion of individuals termed Russian intelligence operatives by the US. However, the Trump administration's tone on the issue has been markedly different and muted.

Such political issues of attribution are bound to have transatlantic effects as well. The same entities connected to *Grizzly Steppe* are also reported to have targeted governmental systems and political organizations in many European countries, including the United Kingdom, the Netherlands, Germany, France and Norway. Unified responses to cyber attacks may be complicated by national political interpretations of their effects. This also risks undermining national declarations of efforts to combat cyber threats.

Conclusion

Cyberspace is a key enabler of a beneficial digital transformation of society, while also bringing with it a new set of risks that need to be properly managed. From an offensive and defensive standpoint, the cyber domain should be understood as an enabler of various types of effects – including profoundly strategic ones.

Europe is already in the midst of an information struggle, in both the technical and the psychological sense. A unified recognition of this fact seems to remain elusive, however. As Mika Aaltola has noted, cyber operations can be used as a synergic tool for influence and destabilization operations.[14] In Europe, there is a need to develop a comprehensive understanding of the model of Russian influence operations utilizing cyberspace, taking into account the non-cyber aspects of the whole operation and their strategic goals. In other words, the effects and responses may not reside solely in the cyber domain, but likely require responses from various types of governmental and non-governmental entities in order to counter and mitigate them effectively.

Given the turbulent political situation in the United States and in European countries, there is a risk that the topic of Russian cyber-enabled influence campaigns will be sidelined in favour of other more pressing concerns, particularly among the larger nations. The European nations on the Eastern flank in particular should remain active in keeping the issue at front of mind, and in finding common ways to react to it.

Key competence in the field of cybersecurity also resides in the private sector. It should also be noted that smaller actors can compete in this space – scale is a factor in computing and network resource

12 'Cyber Special Forces: An Interview with Dmitri Alperovitch', Spycast [podcast], International Spy Museum, 10 January, 2017, https://www.spymuseum.org/multimedia/spycast/episode/cyber-special-forces-an-interview-with-dmitri-alperovitch, accessed 13 February, 2017.

13 T. Rid & B. Buchanan, 'Attributing Cyber Attacks', *Journal of Strategic Studies*, Vol. 38, 2015, p. 7.

14 M. Aaltola, 'Cyber Attacks Go Beyond Espionage: The Strategic Logic of State-sponsored Cyber Operations in the Nordic-Baltic Region', *Finnish Institute of International Affairs*, Briefing Paper 200, 29 August, 2016, http://www.fiia.fi/assets/publications/bp200.pdf, accessed 13 February, 2017.

availability, but this power can be harnessed with a small talent pool. This creates opportunities for Nordic and Baltic companies, for example in harnessing advances in the artificial intelligence field to solve cybersecurity problems. Governments in these countries should nurture and encourage the growth of such potential.

In the Nordic-Baltic context, the smaller population size can also be turned into an advantage in terms of agility. Coordinating responses within government and between different actors can potentially be achieved with less friction and faster than in larger governments with more internal stakeholders and external interfaces. Exposing and being transparent about cyber attacks and influence operations targeted against open democratic societies is necessary to provide evidence for the public about the state of international relations, and to build the case for imposing sufficient costs across domains to deter further operations against sovereign states.

Addressing state-sanctioned influence operations and attacks against individuals will require new thinking by governments, in both preventive and reactive terms. Particularly when it comes to online communities such as those in social media, the responses need coordination not just with governmental but also with commercial entities, such as service providers. Some responsibility must lie with governments to provide protection for their citizens against attacks by state-sponsored actors, which may originate in the digital domain, but have substantial effects in the real world. The case also needs to be made to citizens about how cyber intelligence capabilities can protect the public, the free press, and democratic institutions. This is the case in Finland in particular, where intelligence legislation has not yet been enacted, but would create the foundation for providing protection against nation-state threats in cyberspace as well.

The vulnerability of political actors and decision-makers to malicious state-sponsored attacks utilizing the social reach of cyberspace poses a threat to the proper functioning of government and society. Just as states do not tolerate violence against their citizens by foreign governments, they should not stand idly by when their citizens are being targeted by intrusive and coercive actions through cyberspace. The challenge will lie in the ability of governments to recognize these threats, and in overcoming the political hurdles of attribution. If attackers continue to perpetrate cyber-enabled campaigns with impunity, they will be implicitly incentivized to continue their malicious acts.

The Finnish Institute of International Affairs
tel. +358 9 432 7000
fax. +358 9 432 7799
www.fiia.fi

ISBN 978-951-769-529-9
ISSN 1795-8059
Language editing: Lynn Nikkanen.
Cover photo: Pixabay

The Finnish Institute of International Affairs is an independent research institute that produces high-level research to support political decision-making and public debate both nationally and internationally.

All manuscripts are reviewed by at least two other experts in the field to ensure the high quality of the publications. In addition, publications undergo professional language checking and editing. The responsibility for the views expressed ultimately rests with the authors.

This publication is part of a research project conducted by the Finnish Institute of International Affairs entitled Finland and the Tightening Competition in Global Politics. The project is part of the implementation of the Government Plan for Analysis, Assessment and Research for 2016.