Northern European Cyber Security in Light of the Ukraine War

by
Jarno Limnéll

Chapter 16 in
Kenneth Geers (Ed.), Cyber War in Perspective:
Russian Aggression against Ukraine,
NATO CCD COE Publications, Tallinn 2015

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Finnish Professor Jarno Limnéll, in Chapter 16, discusses the ramifications of the Ukraine war, and its cyber component, for Russia's neighbours. Moscow's aggressive behaviour in Ukraine has forced many countries to re-evaluate their political and military relationships, especially with NATO. For historical reasons, Finland and Estonia are well positioned to analyse Russia's use of hybrid warfare, including information operations. Today, these countries are actively pursuing ways to bolster their national defences against Russia's military strategies and tactics in Ukraine. The NATO Alliance should take concrete measures to reassure its member states, such as the creation of a common cyber defence framework.

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Northern European Cyber Security in Light of the Ukraine War

Jarno Limnéll
Aalto University

1 Introduction

The Ukraine war is a game changer in the international security environment, and its ramifications in Northern Europe are profound. Numerous countries in the region feel that their national security is directly threatened, especially those bordering Russia. New NATO members Estonia, Latvia, Lithuania, and Poland are seeking concrete forms of reassurance from Washington and Brussels, while non-members like Sweden and Finland have reinforced their ties with the NATO Alliance. The Nordic and Baltic countries have sought a closer partnership during the Ukraine war, and this has created an opportunity to advance their regional cyber security dialogue.

Received wisdom states that small countries, especially those located next to a big country, are most at risk when international security breaks down, and that big states do what they want while small states do what they must. During the war in Ukraine, northern European countries have been forced to re-evaluate their relationship with NATO as well as their preparedness against Russia's 'hybrid warfare' which blends conventional and unconventional operations, regular and irregular tactics, information warfare, and cyber warfare. Cyber threats in particular have been an integral part of these ongoing discussions, as northern European countries have been subjected to various forms of cyber attack during the Ukraine war.

This chapter concentrates on two of Russia's neighbours that have always been in the 'realist' camp in term of their national security policy: Finland and Esto-

nia. The response of each nation to the Ukraine crisis has been different, reflecting their traditional approaches to foreign and security policy as well as their existing ties to NATO. Yet these two nations have much in common: a fundamental interest in regional stability, Western unity, a norms-based view of international order, interdependence, and an essential need for cooperation in the field of foreign and security policy. These same principles drive both nations' prevailing views on both information security and cyber security – two issues which are sometimes distinct, and sometimes closely related.

2 Finland: Coming to Terms with Hybrid Warfare

'Is Finland really getting ready for war with Russia?' An American news channel posed this question in May 2015, when nearly a million Finnish military reservists received letters detailing their assigned duties in a crisis situation.[1] In fact, the correspondence was unrelated to Russia's annexation of Crimea or its ongoing war in Ukraine, but the media attention that this event generated speaks volumes about the age-old nature of the Russo-Finnish relationship.

Historically, Finland´s national security strategy has almost exclusively been focused on Russia, and Finns have been following the war in Ukraine extremely closely. From the beginning, Finland has condemned Russia´s activities in its largest European neighbour. Finnish President Sauli Niinistö summarised the current situation well: 'We have a long history with Russia — not that peaceful all the time. So everything the Russians are doing, surely the Finns notice and think very carefully about what that might mean'.[2] Defence Minister Carl Haglund was more direct in his choice of words: 'Russia says one thing but does another. I do not trust Russia at all'.[3]

The concept of 'cyber' is rather new in the Finnish language.[4] It was institutionalised in 2013, when Finland published its *National Cyber Security Strategy*, which described cyber security as 'the desired end state in which the cyber domain is reliable and in which its functioning is ensured'.[5] Public discussion of the importance of cyber security is a natural outgrowth of Finland being one of the most advanced information societies in the world, a country that relies heavily on the proper functioning of myriad electronic networks and services. For years, there has been an active societal debate in Finland on topics such as public-private partnerships in cyberspace, the need for better legislation, the development of cyber defence capabilities within the Finnish Defence Forces, and much more.

1 Holly Ellyatt. 'Is Finland really getting ready for war with Russia?'*CNBC*, May 25, 2015.
2 Griff Witte. 'Finland feeling vulnerable amid Russian provocations,' *The Washington Post*, November 23, 2014, 6.
3 Gerard O'Dwyer. 'Finland Brushes Off Russian Overtunes,' *DefenseNews*, February 15, 2015, http://www.defensenews.com/story/defense/international/2015/02/15/finland-russia-border-relationship/23301883/.
4 Jarno Limnéll. 'Kyber rantautui Suomeen,' *Aalto University Publication Series 12/2014*, Helsinki 2014. Concepts like information security or computer security have been used for decades in the Finnish language.
5 Secretariat of the Security Committee, *Finland´s Cyber Security Strategy*, Government Resolution 24.1.2013, 1.

In Finland, there has been intense analytical focus on Russia´s traditional warfare capabilities (including in Ukraine), but there has been limited discussion regarding Russia's cyber activities. Finnish analysts have noticed Russian cyber espionage in Ukraine, Distributed Denial-of-Service (DDoS) attacks against Ukraine, and the disruption by pro-Russian hackers of Ukrainian media and telecommunications networks.[6] However, most Finnish cyber experts have been surprised that cyber attacks have not played a greater role in the conflict, and frankly, we expected to see more. According to our analysis, the primary reason for this is likely that Ukraine is simply not a very cyber-dependent country; therefore, Russia could better fulfil its national security agenda by other means, as cyber attacks may not have the desired effect. As a consequence, it has not been necessary for Russia to use its more strategic cyber capabilities.

It has not been necessary for Russia to use its more strategic cyber capabilities.

In Finland, one change has been a deeper appreciation of the seriousness of cyber espionage, and this is partly due to Russia´s cyber activity in Ukraine. For the first time, Finland has accused Russia of carrying out intelligence activities – both physical and cyber – within its territory. In the past, Finnish Security Police reports had only vaguely mentioned that some 'foreign countries' had engaged in espionage against Finland.

Cyber threats from Russia have been viewed in Finland primarily in the context of 'hybrid' warfare, which is understood in Finland to be a more intelligent or efficient way to wage war because it seeks to achieve political goals without the extensive use of traditional violence. Using a range of tools such as cyber attacks, economic pressure, information operations, and limited physical attacks to generate uncertainty in the mind of the general population, an aggressor may be able to achieve its desired political goals.

In Finland, it is understood that modern Russian warfare puts great emphasis on cyber and electronic warfare. In particular, Russian activities in Ukraine have spurred Finland to strengthen its military and societal defences. The new Finnish Government programme puts it this way: 'The Government will strengthen the comprehensive concept of security nationally, in the EU and in international cooperation. This applies, in particular, to new and large-scale threats, such as the defence against hybrid attacks, cyber attacks and terrorism'.[7]

From a Nordic perspective, one of the most alarming aspects of the Ukraine crisis has been Russian attempts to wage information warfare to influence public opinion. Finnish media – and even ordinary Finns – have discussed this dynamic in detail. Even the Finnish Prime Minister has openly stated that there is an ongoing

6 Jarno Limnéll. 'Ukraine crisis proves cyber conflict is a reality of modern warfare,' *The Telegraph*, April 19, 2014, http://www.telegraph.co.uk/technology/internet-security/10770275/Ukraine-crisis-proves-cyber-conflict-is-a-reality-of-modern-warfare.html.

7 Prime Minister´s Office, *Strategic Programme of Prime Minister Juha Sipilä's Government*, Government Publications 12/2015, May 29, 2015, 38.

information war in Ukraine. Finns have noted pro-Russian 'trolling', or the aggressive use of online arguments and false information toeing the Kremlin line. Such tactics increased significantly as the Ukraine crisis escalated.[8] In the flood of Finnish, English and Russian troll messages, the same phrases are constantly repeated: Russia and President Vladimir Putin are idolised and the military operations of Russia in Ukraine are justified – or simply denied. The Russian Embassy in Helsinki has active Facebook and Twitter accounts; on Twitter, @russianembfinla has retweeted pro-Russia trolls and the (often anonymous) tweets of anti-Western voices, blocked Finnish journalists critical of Russia, distributed photos of Ukrainian civilian casualties, and altered the messages of Finnish tweeters.

> *One of the most alarming aspects of the Ukraine crisis has been Russian attempts to wage information warfare to influence public opinion.*

There are numerous vexing challenges. For example, it is difficult to prepare countermeasures for an attack that is outsourced to hacker groups that lie outside normal state structures. In Ukraine, these are theoretically separatist groups in Crimea and eastern Ukraine. Cyberspace is the ideal place to wage anonymous – or at least plausibly deniable – operations.

For Finnish defence planning, the increased use of hybrid warfare does not mean forgetting more traditional military threats to our nation, but it does complicate matters – especially societal preparedness. Cyber attacks are now an integral part of all conflicts and wars, and they are blurring the line between peace and war. As Finland´s President Niinistö stated:

> *'With hybrid warfare, we are facing a substantial change in military operations. The boundary between actual war and other exercise of power is becoming blurred. Means of cyber war and information war are becoming increasingly important. It is now possible to fight a war without actually being at war. At the same time, conflict escalation is setting new speed records, as we saw for instance in the Crimea.'*[9]

3 Estonia: Cyber Attacks and NATO Article 5

In 2007, Estonia became the first country in the world to be targeted by a coordinated international cyber attack which came in retaliation for Tallinn's decision to relocate a World War II monument from the centre of Tallinn to a military cemetery

8 Finland's national public-broadcasting company YLE gathered a large amount of information on pro-Russia trolling. 'Yle Kioski Investigated: This is How Pro-Russia Trolls Manipulate Finns Online – Check the List of Forums Favored by Propagandists,' last modified June 24, 2015. http://kioski.yle.fi/omat/troll-piece-2-english.

9 Speech by President of the Republic Sauli Niinistö at the ambassador seminar, August 26, 2014. http://www.presidentti.fi/public/default.aspx?contentid=311373&nodeid=44807&contentlan=2&culture=en-US.

on the outskirts of the city. Today, Estonia is considered to be a world leader in all things digital, including cyber security.[10] Estonia's current *Cyber Strategy* notes that the environment is growing more dangerous: 'The amount and activeness of states capable of cyber-attacks are increasing'.[11]

Estonia has been subjected to pressure from Moscow for years, but Russian cyber espionage in Estonia's government and commercial affairs is also getting worse. Therefore, when tensions began to rise in Ukraine, Estonia was one of the first nations to sound the alarm. In late 2014, Estonia´s Prime Minister Taavi Rõivas declared that '[w]e, in Estonia, fully understand that challenges may arise from other directions, including in the cyber domain'.[12]

Russian´s annexation of Crimea has raised fears in the Baltic states that they could be the next victims of Russian aggression. In all three countries, there are many people alive today who personally witnessed Russian tactics similar to those now on display in Ukraine. Both Latvia and Estonia have large Russian-speaking minorities living within their borders.

Estonia is different from Finland in one key regard – its NATO membership. Estonia´s President Toomas Hendrik Ilves is an active figure in NATO security and policy circles, particularly those that relate to cyber: 'Shutting down a country with a cyberattack would be very difficult but not impossible. If you did that, why wouldn't that be a case for Article 5 action?' Article 5 of the NATO Charter states that any attack on one member of the Alliance can be viewed as an attack on all. At the NATO Wales Summit in 2014, in part due to Ilves´s tireless work, NATO ministers ratified a policy stating that not only conventional and nuclear attacks, but also cyber attacks, may lead to an invocation of Article 5.[13,14]

In the past, a NATO ally under cyber attack could convene a group to consult on the attack, but not call on allies to respond in any way. With cyber attacks now falling under Article 5, NATO members now have the option of doing so. This is a major shift in policy, given that cyber warfare is still largely shrouded in mystery and secrecy. National cyber capabilities tend to be highly classified. Therefore, despite differing capabilities, viewpoints, and thresholds (after all, what Estonia might consider to be an intolerable assault on its sovereignty might not be seen the same way in Brussels or Washington) this was a significant event in that a public announcement that NATO might respond to a cyber attack as it would to a kinetic or traditional attack has tangible value in the realm of international military deterrence.

During the conflict in Ukraine, DDoS attacks against Estonia have been surprisingly few. In fact, despite expectations, the past year has been unusually calm

10 According to the global cyber security index of the International Telecommunication Union (ITU), Estonia is ranked fifth in the world in the field, and according to the recently published Business Software Alliance (BSA) report, Estonia, Austria and Netherlands are the most cyber-secure countries in Europe.

11 Ministry of Economic Affairs and Communications, *Cyber Security Strategy 2014-2017*, 2014, 5.

12 Ashish Kumar Sen. 'Estonia´s Prime Minister: NATO Presence Key to Counter Russia´s Provocations,' *Atlantic Council*, December 11, 2014.

13 NATO, 'Wales Summit Declaration,' September 5, 2014. http://www.nato.int/cps/en/natohq/official_texts_112964.htm.

14 E.g. Roger Boyes. 'NATO must respond to Russian cyber assault,' *The Times*, April 3, 2015.

compared to the previous year.[15] In 2013, the level was much higher: for example, the websites of the Ministry of Defence and the Estonian Defence Forces were both hit by DDoS, for which responsibility was claimed by 'Anonymous Ukraine'.[16] Also in 2013, the website of Estonian railway company *Elron* (which happens to be the most popular Google search term in Estonia) was defaced with messages claiming that passenger train traffic had been halted as a result of a NATO military exercise.[17] Earlier the same day, the website of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) came under DDoS attack (Anonymous Ukraine again claimed responsibility). At NATO Headquarters in Belgium, several websites have been targeted during the Ukraine war, as well as NATO's unclassified e-mail system. NATO officials have described these attacks as serious assaults, but also said that they did not pose any risk to NATO´s classified networks.[18]

The hacker group 'Cyber Berkut' said the attacks were carried out by patriotic Ukrainians angry over NATO interference in their country, and also stated that NATO CCD COE experts had been in Ukraine training 'cyber terrorists'. Although attribution of cyber attacks to specific actors and nations is difficult, technical analysis of the Cyber Berkut's domains as well as the nature of its propaganda strongly suggest ties to Russia.[19]

Since the beginning of 2014, however, Estonian cyberspace has been unusually calm. Like Finland, Estonia has seen espionage, pro-Russia trolling on Estonian web forums, and propaganda, but little in the way of malware or computer exploits. Estonians feel that the 'hostile information flow' from Russia is aimed at creating and widening rifts between native Estonians and ethnic Russians (Moscow does not see normal relations as beneficial to its current foreign policy). For example, on 4 March 2015, the television channel *Rossiya-1* (a key source of information for many ethnic Russians in the Baltic region) aired a satirical anti-Nazi video that was said to be 'proof' of Estonia's support for Nazism.[20] In response, Estonia will create its own Russian-language TV channel, to be launched in September 2015 by a state-financed public broadcaster, that will seek to empower the local ethnic Russian identity.[21]

A NATO member only since 2004, Estonia today occupies a highly visible position within the Alliance. Thus, the hybrid military campaign that Russia has launched in Crimea and in eastern Ukraine almost forces NATO to take proactive steps to guard against the use of such tactics in the Baltic states, if not to rethink some of its defence strategies altogether. As Estonia´s Defence Minister Sven Mikser stated, 'We have reason to believe that Russia views the Baltic region as one

15 Private conversations with Estonian officials.
16 CERT-EE kokkuvõte, 'Hajusad ummistusründed, võltsitud saatjaga e-kirjad ning näotustamised 1.-7. Novembril 2013, aka #OpIndependence,' https://www.ria.ee/public/CERT/opindependence.pdf.
17 E.g. Ronald Liive. 'Väide Regnumilt: NATO suurõppuse käigus rünnati ekslikult ehtsaid veebilehti,' *Forte*, November 13, 2013.
18 'NATO websites hit in cyber attack linked to Crimea tension,' *Reuters*, March 16, 2014.
19 Rodrigo, 'Cyber Berkut Graduates from DDoS Stunts to Purveyor of Cyber Attack Tools,' *Cyber Threat Intelligence*, June 8, 2015. https://www.recordedfuture.com/cyber-berkut-analysis/.
20 Ott Ummelas. 'Estonia Must Counter Hostile Russian Propaganda,' *Bloomberg Business*, March 25, 2015.
21 Silver Tambur. 'EER's new Russian-language TV channel will be called ETV+,' April 20, 2015.

of NATO's most vulnerable areas, a place where NATO's resolve and commitment could be tested'.[22]

Today, cyber security is increasingly seen as playing a vital role in national security affairs, both in and out of NATO. For its part, Estonia is already sharing its cyber security experience and expertise with Ukraine, including the organisation of large cyber security drills. And finally, Estonia has one major advantage on its side: it is home to the NATO CCD COE, whose symbolic importance to Estonia has grown rapidly.

4 Conclusion: David vs. Goliath in Cyberspace

Finland and Estonia both rank among the world's most connected and cyber security-savvy countries.[23] In both nations, there is a high degree of dependence on the internet, as well as a deep appreciation for the strategic nature of modern networks and the need to secure them. Therefore, both Finland and Estonia are at the forefront of the nations creating cyber norms in the world.[24]

The need to prepare defences against modern hybrid warfare forces governments, including those of Finland and Estonia, to take steps sooner rather than later. There will be conflicts in which the regular armed forces of a foreign state are not the most active participants. Some of the attacks may occur entirely in cyberspace, and the attackers might even remain anonymous. In the internet era, a wide range of national laws must be re-examined and contingencies rehearsed, so that decision-makers have the best possible tools to respond to the challenges of hybrid warfare in the future.

Russia is far larger and more populous than both Finland and Estonia, but traditional notions of size – especially in the globalised internet era – is not the only determining factor on the cyber battlefield. Smaller countries such as Finland and Estonia, with a strong heritage of technical capability and experience, may possess some advantages that not even great powers could dream of. In the near term, Finland will continue to strengthen its defences independently, while Estonia will continue to emphasise NATO´s Article 5. In the long term, Finland and Estonia will continue to punch above their weight in the cyber domain – especially relative to their size.

Smaller countries with a strong heritage of technical capability and experience may possess some advantages that not even great powers could dream of.

22 Geoff Dyer. 'NATO shifts strategy in Europe to deal with Russia threat,' *Financial Times*, June 23, 2015.

23 *Global Cybersecurity Index and Cyberwellness Profiles*. International Telecommunications Union, April 2015 http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf.

24 See e.g. Jarno Limnéll. 'Can Finland Act As a Mediator on Cyber Norms?' *Council on Foreign Relations*, May 28, 2015, http://blogs.cfr.org/cyber/2015/05/28/can-finland-act-as-a-mediator-on-cyber-norms/.