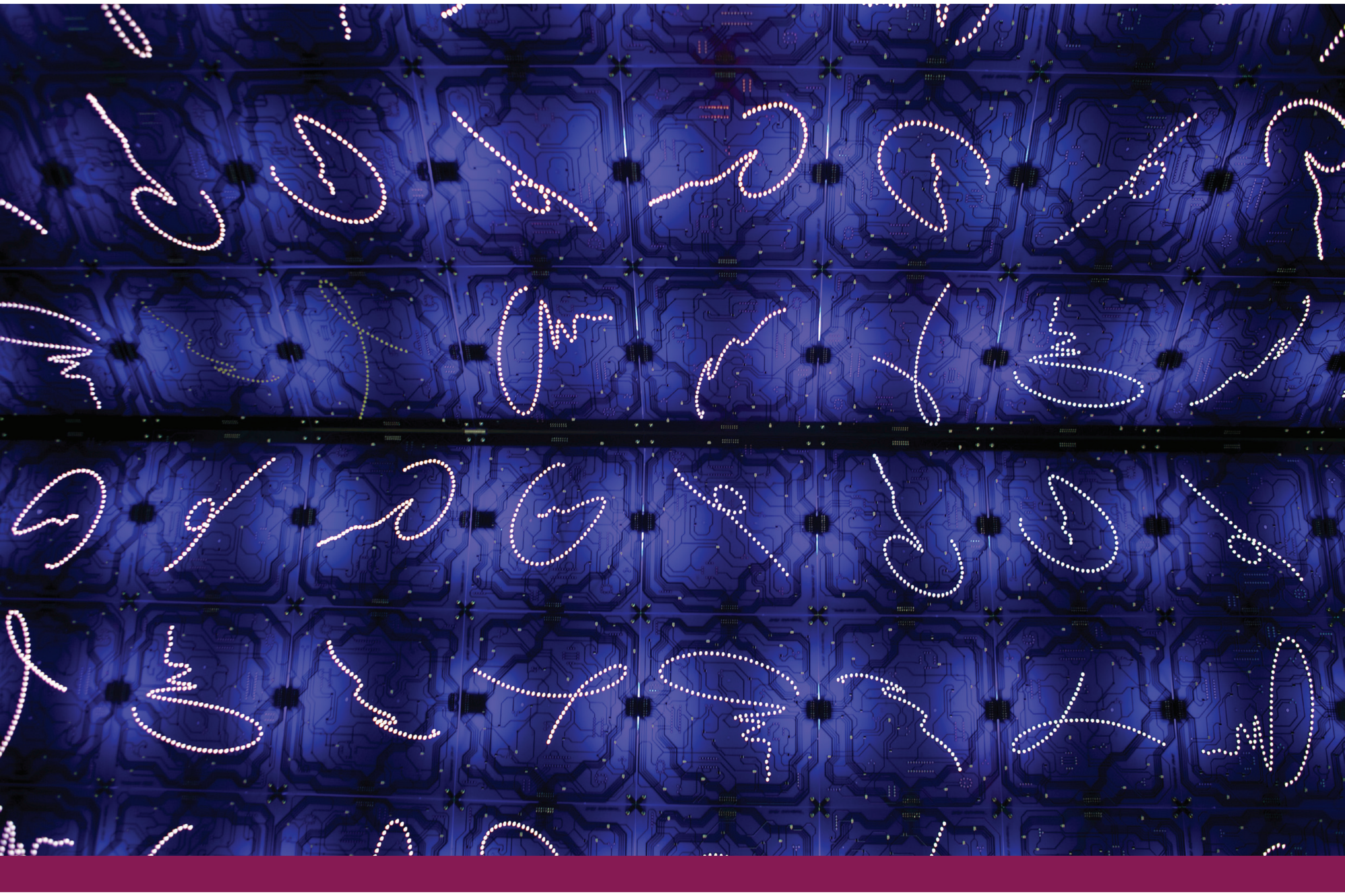
CYBER ATTACKS GO BEYOND ESPIONAGE

THE STRATEGIC LOGIC OF STATE-SPONSORED CYBER OPERATIONS IN THE NORDIC-BALTIC REGION

Mika Aaltola

FIIA BRIEFING PAPER 200 ▪ August 2016



ULKOPOLIITTINEN INSTITUUTTI
UTRIKESPOLITISKA INSTITUTET
THE FINNISH INSTITUTE OF INTERNATIONAL AFFAIRS

CYBER ATTACKS GO BEYOND ESPIONAGE

THE STRATEGIC LOGIC OF STATE-SPONSORED CYBER OPERATIONS IN THE NORDIC-BALTIC REGION

Mika Aaltola
Programme Director
Global Security Research Programme
The Finnish Institute of International Affairs

FIIA Briefing Paper 200
August 2016

- As the Nordic-Baltic region has digitized its critical infrastructures and decision-making processes, awareness of the resulting geopolitical vulnerabilities has lagged behind.

- There is a need to understand that cyber operations have strategic aims that go beyond mere snooping and spying. They are effective at spreading mistrust, blackmail, and destabilization, and at showcasing the perpetrator's capabilities and serving its deterrence purposes.

- The harm scales used to evaluate the severity of a cyber attack usually focus on physical or economic damage, overlooking the real significance of politically-motivated cyber attacks. For example, the damage caused by rigging an election process goes far beyond some of the physical harm scenarios.

- Cyber operations are particularly effective in combination with other political pressuring tools. The spectrum of these combinatorial tools is still relatively restricted. Yet the worrying aspect is that this synergic spectrum can widen and lead to cyber escalation, in which case the level of harm caused by the cyber operations will become higher and more prolonged, especially in the (geo)-political sense.

- It remains to be seen whether a higher state of cyber resilience can be achieved without active means for cyber deterrence such as stronger political shaming, economic sanctions, or active cyber deterrence-building.

ULKOPOLIITTINEN INSTITUUTTI
UTRIKESPOLITISKA INSTITUTET
THE FINNISH INSTITUTE OF INTERNATIONAL AFFAIRS

Recent years have seen an increasing number of geopolitically-motivated cyber attacks in the Nordic-Baltic region. These have included the so-called Dukes – a family of Russian-originated malware programs – and the Red October and Turla large-scale cyber-espionage campaigns. The targets have included governmental offices and international organizations in several countries.

Three main factors are driving these cyber activities in the Nordic-Baltic region: First, trade espionage against the region's advanced innovation economies and large portfolios of intellectual property; and second, information-gathering through the links that the region's states have with wider institutions and security organizations. Thirdly, new uses that have been found for cyber operations – that is, they can be used as a synergic tool for influence and destabilization operations in regional organizations, as well as in individual countries of the region.

A broad and well-developed innovation economy increases the likelihood of illicit cyber activities against commercial entities. Rewards become higher and incentivize the use of more advanced and sophisticated hacking techniques. The Nordic-Baltic states are high-opportunity targets for cyber spying. In particular, the intellectual property of the region's communications technology, energy, shipping, bio-technology, and defence sectors provides the motivation for cyber-enabled theft. Furthermore, the illicit interest of an external commercial actor and its host state can align in a spectrum of different types of illicit activities – especially in the case of more centralized and unitary political actors.

What is true of stealing industrial property can also apply to geopolitically-motivated cyber activity. State secrets are largely online and key influence networks can be mapped out and accessed through digital channels. There are obvious geostrategic reasons why the region is interesting for different combinations of state and state-sponsored entities. For example, it is clear that the close relations of the region's states with international institutions (e.g. the EU, NATO, or the Arctic Council), some security processes (e.g. the integrating defence policies in the region), or certain influential events and decisions, such as national elections, referendums, high-level meetings or Nobel Committee decisions, are highly interesting for outside actors.

Further, as geopolitical tensions have worsened since the occupation and annexation of Crimea in 2014, the region has become a target for disinformation and influence operations. Possible reactions by the states in the region to the growing sense of insecurity as well as potential realignments are under intense scrutiny. Due to these heightened external motivations, the Nordic-Baltic states are increasingly exposed through – and because of – their developed and connected information technological networks.

The geopolitics of cyber asymmetries

Cyber connectivity is clearly unevenly spread. The United States, Western and Northern Europe, and some parts of East Asia are highly connected and hence vulnerable and exposed to cyber hacking. A noteworthy fact is that all the Nordic states are among the top seven in the network readiness index published by the International Telecommunication Union (ITU), which measures the percentage of the population that is connected to the internet. The Baltic states have also made considerable progress in adopting digital technologies. These Nordic-Baltic achievements are, paradoxically, also measures of high opportunity cost. In other words, the clear advantages have a downside in terms of cyber vulnerability.

In many cases, the control mechanisms of critical infrastructures and decision-making processes have been fully digitized. This increases the benefits for hackers, and makes it more likely that the strong cyber modality will be used as an attack vector in intelligence-gathering and influence/destabilization operations instead of other more traditional avenues.

On the other hand, it should also be taken into consideration that the Nordic-Baltic states are not evenly matched in terms of digitization and preparedness when it comes to cyber vulnerabilities, awareness and cyber-defence capabilities. Estonia, having experienced widespread attacks before, has taken the lead in developing capabilities and solutions through the NATO Cooperative Cyber Defence Centre of Excellence, which was established in Tallinn in 2008. Finland and Sweden are also participating in the work of the Centre, which aims to enhance the capability, cooperation and information-sharing in cyber defence. Some of the capabilities are also high in Sweden, whose legal framework allows for wider cyber surveillance than in many other states. The states in the region are developing and sharing their cyber security capabilities through networked arrangements.

In addition to the connected physical ICT, the states in the region have for years based their national strategies on the centrality of being members of multiple regional and international institutions and alliances. They are institutionally very well linked, and possess institutional leverage and capital. This positive depth of institutional engagement means that the states offer attractive access points to confidential and secret information on regional and international institutions. The connected physical ICT in combination with the highly digitized decision-making processes and regional institutional capital increase the expected rewards from illicit cyber activities.

However, an often ignored aspect of cyber operations is that they can also be used to test preparedness and accentuate a sense of vulnerability in the target countries. The likelihood of being a target of sophisticated cyber hacking is a function of the possible rewards in terms of useful intelligence on the state's relations with the key organization. It can be suggested that heightening the target state's sense of cyber vulnerability is useful in influencing its engagement with the key institutions. Targeted cyber hacking can be used to signal displeasure, it can lead to hesitation in the target states, and, at a practical level, it can complicate everyday communication and decrease the sense of confidentiality and trust.[1]

A heightened sense of vulnerability can condition a target state to be less likely to support policies that it perceives as contrary to the interests of the cyber perpetrator. This conditioning effect is heightened when there is a clear perception that the perpetrator can escalate its illicit cyber activities depending on the policies adopted. In some respects, cyber hacking functions as a signalling and alerting operation in the same way as military airspace violations or maritime harassment.

This conditioning/blackmailing effect works optimally when three conditions are created: High expectations concerning future cyber escalations and clear past cases when the perpetrator has been able to take advantage of cyber vulnerabilities; widespread awareness of extensive vulnerabilities in one's own critical digitized systems; and a strong belief in the suspected state's strong determination and sophistication in illicit cyber operations.

The most crucial component, however, is the role that cyber operations can play in tandem with other means of pressure such as corruption operations, geoeconomic pressure, election manipulation operations, disinformation campaigns or military manoeuvres. Geopolitically-motivated cyber operations seldom happen in a vacuum where other types of operations are not being carried out.[2]

The identity of a geopolitical cyber perpetrator

The attribution of actual cyber attackers is usually regarded as extremely tricky, as the perpetrator can use various means to cover its tracks. The range of possible actors is wide, from single individuals to criminal groups, loose hacker networks, and state actors. However, the Nordic-Baltic states have relatively sophisticated ICT security systems. This means that geopolitically-motivated cyber operations most often require both determination and skills that only a few non-state and state-level actors possess. The underlying characteristics of the region's systems can be used to overcome the usual attribution problems.

The uneven geographical spread of connectedness reveals the general intentionality and directionality of geopolitically-motivated cyber operations. The perpetrators are most likely major states with high deterrence capabilities. They are more determined

[1] E.g. http://www.reuters.com/article/us-ukraine-nato-idUSBREA2E0T320140316; https://en.wikipedia.org/wiki/Columbian_Chemicals_Plant_explosion_hoax; https://twitter.com/bellingcat/status/702395665201176576, all accessed 26 August 2016.

[2] E.g. the use of the BlackEnergy malware family against the critical infrastructure of Ukraine. It is suspected of causing a power outage in Western Ukraine just around Christmas 2015, and it was also detected in the networks of Kiev international airport in early 2016.

as they risk facing the political consequences of getting caught. They have conventional and cyber deterrence and are therefore less likely to face any adverse consequences if the illicit activities are uncovered. A more detailed profile of a geopolitical cyber attack includes the following attributes:

1. Need for institutional access: States that lack institutional access and that are motivated to use the states in the region as an access point to some of the key institutions (e.g. the EU or NATO) and to privileged information.

2. (Un)desirable realignment: States that have the most to lose vis-à-vis the possible re-orientation or changing status of the states in the region, or have the most to gain from such a change or non-change. Nordic non-NATO members Finland and Sweden in particular can be seen as key targets of these state-sponsored hacking activities.

3. Sophisticated capabilities: The perpetrators are likely to have deep knowledge of the target's technical vulnerabilities, which is usually not very hard to obtain. Another requirement is knowledge of what happens inside the systems once the attack is deployed and how to exploit a specific vulnerability for one's own ends.

4. Mass-surveillance capability: Besides the more targeted individual cyber hacking cases, there are cyber-based mass-surveillance activities that are carried out by major states, for example by tapping into the undersea cables running across the Baltic Sea. Such wider surveillance can give a perpetrator a broad understanding of the regional and country-specific dynamics and how to promote and benefit from discord and instability within the respective societies or among the states.

5. Destabilization motivation: A likely perpetrator has the motivation to increase the sense of insecurity and vulnerability in the Nordic-Baltic region, and to cause discord and the emergence of differential national interests inside the region.

The greater the political rewards derived from cyber attacks, the more likely is the use of complicated and sophisticated cyber tools. In the region, this likelihood is increased by the fact that the states have comparatively better ICT capabilities and more effective security systems.

The Duke and Red October operations

There have been three notable recent waves of cyber attacks in the Nordic-Baltic region: The Duke malware family and the Red October and Turla campaigns.

For example, a four-year-long cyber espionage campaign against the systems of the Finnish Foreign Ministry was uncovered in 2013. The malware managed to infiltrate the Foreign Ministry's computers and went undetected for many years. It was not noticed until a tip was received from the Swedish National Defence Radio Establishment. The tools used were similar to, but more sophisticated than what was used in the so- called Red October campaign, which had lasted since 2007.[3] The campaign had utilized a version of a computer worm called Agent.btz, which has been around since 2007 and which was also utilized in the so-called Turla cyber espionage campaign. There are indications that the Red October and Turla campaign and the Agent.btz worm are all interconnected by their developers or by the state of origin.[4] The apparent target was Finland's communications and networks with the EU. The first versions of these campaigns infected US military systems in 2008 in a severe incident, and it was partly due to this infiltration that the US decided to establish its US Cyber Command.[5]

There are several strong indications that these attacks, targeting many Western European and North American institutions over multiple years, were perpetrated by an actor inside the Russian

[3] YLE, "Venäläisen verkkovakoojan 12 askelta Suomen ulkoministeriön koneille ja jälkien peittämiseen", http://yle.fi/uutiset/venalaisen_verkkovakoojan_12_askelta_suomen_ulkoministerion_koneille_ja_jalkien_peittamiseen/8591034, 13 January 2016, accessed 26 August 2016.

[4] Reuters, "Suspected Russian Spyware Turla targets Europe, United States", http://www.reuters.com/article/us-russia-cyberespionage-insight-idUSBREA260YI20140307, 7 March 2014, accessed 26 August 2016.

[5] Kaspersky, "How Turla and 'worst breach of U.S. military computers in history' are connected", http://www.kaspersky.com/about/news/virus/2014/How-Turla-and-worst-breach-of-US-military-computers-in-history-are-connected, 12 March 2014, accessed 26 August 2016.

government or very close to it.[6] According to many experts, the illicit activity was organized and financed by a state actor and much of the evidence points to Russia.

A second notable case of state-sponsored cyber attacks in the Nordic-Baltic region concerns the Duke campaigns. These persistent attacks have used a group of information-stealers, or Dukes: MiniDuke was used to attack European government organizations and NATO, CosmicDuke was active during 2014 and, recently, CozyDuke targeted the White House and US Department of State. Other targets have included the ministries of defence in Georgia and Estonia, foreign ministries in Turkey and Uganda, and political think tanks in the US, Europe and Central Asia.

Dukes typically infect a computer through an email containing a link or a decoy attachment; opening them establishes backdoor access to the victim's system. Although the Dukes are different, they share some features (e.g. the loader) and bear a family resemblance that is also indicated in the naming scheme.[7] The shared features of these attacks have led to speculation concerning the perpetrator(s) behind them.

However, the attribution of a cyber attack can easily be misdirected. One can hide the true identity of the perpetrators, for example by using third parties as attack vectors, by using common identifying markers, or by leaving misleading 'hints' within the code. The 'fog' is further increased by engaging in deceptive targeting of something other than the real geopolitically-motivated targets. The actors can also engage in a variety of methods.

Despite the inherent obscurity and diversions, repeated attacks leave better markers of identification: first, the signature of intended targets becomes clearer; second, cyber attacks are based on human activity, and errors are becoming increasingly detectable; and finally, the forensic tools have improved in ways that could not be foreseen a few years ago. In the Duke case, F-Secure Lab's analysis is, to date, the best evidenced and most detailed investigation into a geopolitically-motivated, state-sponsored cyber operation.[8]

Past research indicates that CozyDuke has been in existence at least since 2011, but the latest analysis provides evidence from 2008 onwards. The list of original targets reinforces the geopolitical intention of the attacks. On the whole, the list of targets concentrates on entities whose interests oppose, are lukewarm towards, or direct negative attention towards Russian geostrategic aims. The pattern of targets over many years can be used to narrow the range of possible perpetrators that are likely to have the persistent intent and necessary capabilities to execute such attacks.

Despite the hype, fuller spectrum is not yet full spectrum

A carefully calculated cyber attack can be useful in a region where a perpetrator has no clear hard power tools. Unlike in Ukraine, in the Nordic-Baltic region, harder means are not directly available at low cost. In this context, the cyber attacks provide the means to create geopolitical reluctance in, and reminders for, smaller states whose possible moves and reorientations might cause a headache for Russia's overall geopolitical aims. The attacks also show the ineffective nature of cyber defence and deterrence in the states in the region. They heighten alarm and create further pressure to acknowledge Russian political insinuations or face the costs of continued attacks and of revamping and reorganizing the existing cyber defences.

The status quo-challenger state can reinforce its claims for a new security arrangement by showcasing the states' strategic weaknesses and vulnerabilities. Demonstrations of these weaknesses are useful not only in the (still unlikely) case of military conflict, but also for the far more likely purposes of

[6] E.g. Wired, "Russian spy gang hijacks satellite links to steal data", http://www.wired.com/2015/09/turla-russian-espionage-gang-hijacks-satellite-connections-to-steal-data/, 9 September 2015, accessed 26. August 2016.

[7] F-Secure, "CosmicDuke: Cosmu With a Twist of MiniDuke", https://www.f-secure.com/documents/996508/1030745/cosmicduke_whitepaper.pdf, 2 July 2014, accessed 26 August 2016.

[8] F-Secure, "The Dukes: 7 years of Russian Cyber-Espionage", https://labsblog.f-secure.com/2015/09/17/the-dukes-7-years-of-russian-cyber-espionage/, accessed 26 August 2016.

demonstrating and catalyzing regional, European and Western senses of vulnerability and insecurity. Carrying out repeated successful attacks creates a sense of power and invulnerability in itself. By using persistent advanced threats, Russia can demonstrate its status as an equal among major powers that have been known to use complex cyber tools for geopolitical ends.

The challenge to the existing regional order inevitably blurs the line between normal and unconventional. What is considered legal, established, and conventional becomes an obstacle as the challenger tries to reset the rules and expectations. This logic increases the possibility of unexpected events in the region. The distinction between peace- and wartime practices can become more blurred. However, there is no evidence of using cyber attacks to cause widespread physical damage in the region; the infrastructure has been outside of the targets.

The US has been employing a harm scale to measure the damage inflicted and also to indicate what counter-measures should be appropriate. The most serious forms of attack can cause harm to major cyber networks or to critical infrastructure by disrupting the national power grid. So far, the attacks have been unlikely to attract clear retaliatory actions. Risks have clearly been taken, but in a calculated way that maximizes the psychological and political effect, but minimizes the chances of punishment. On the other hand, the harm scale that focuses on physical damage misses the real significance of politically-motivated cyber attacks. For example, the damage caused by rigging an election process far surpasses some of the physical harm scenarios.

It is important to realize that even when uncovered, the attacks showcase the perpetrators' capabilities. This can even be useful for the attacker, as its image as a powerful modern actor is highlighted in public discussions. When an operation becomes public, the perpetrators can always point to the attribution issues and deny their role in the operations to delegitimize any retaliation. Perhaps paradoxically, the public revelations about ongoing and active cyber operations can even be part of the overall strategic goal of demonstrating power and the degree of impunity. This is a possibility that the target states/institutions have to take into consideration.

Intended level of harm?

Besides the loss of data, technical dysfunction and economic consequences caused by repairing the damage, an attack can give rise to mistrust and disloyalty, and have political ramifications. In cases where the targets do not know what has been perpetrated, the attack erodes trust towards the state organization and its data. Trustworthiness is a major casualty of the attacks. In the case of the recent attacks, access to the system is gained through someone in the organization opening a falsified email or decoy document. This is likely to be passed on to people outside of the organization. Whether intended or not, such an attack pattern lowers the level of intra- and inter-organizational trust, loyalty, and solidarity.

Successful cyber campaigns, especially when repeated, constitute a form of cyber bullying. The disruptive psychological effect is enhanced by the logic of 'robbing the same bank many times'. Repeated intrusions into the region's institutions lead to a greater sense of vulnerability, sense of lost agency, and unpredictability. Repeated intrusions into the state organization responsible for security test the sense of security, which is the raison d'être for the institutions in the first place.

The recent case of cyber attacks in connection with the US presidential elections is particularly alarming. The apparent hacking of the Democratic Party's and Hillary Clinton's campaign systems seems to have been timed to influence the outcome of the election. The key lesson that should be learned is that open and highly digitized democracies are vulnerable during elections, as the electorates are forming their opinions and the nations are making crucial crossroad decisions. The fast tempos of national elections and referendums do not easily allow enough time to thoroughly investigate illicit cyber activities.[9] Sudden leaks and deceptive tactics can cause election destabilizing scandals and loss of trust in vital democratic institutions or mechanisms. Hence, extra caution should be exercised at different levels during elections in the states in the region.

[9] E.g. Reuters, "Exclusive: Clinton campaign also hacked in attacks on Democrats", http://www.reuters.com/article/us-usa-cyber-democrats-investigation-exc-idUSKCN1092HK, 30 July, 2016, accessed 26 August2016.

The Nordic-Baltic region's main response has been to strengthen deterrence by bolstering cyber security. The systems are in a higher reactive mode. Vigilance has been increased against different types of shocks, disruptions, and attacks. The goal is for systems as a whole to be in a state of resilience, self-monitoring, and self-repair. However, the question remains: Can such a high state of resilience be achieved without active means of cyber deterrence such as strong shaming, economic sanctions or cyber counter-attacks? It is likely that the game will continue whereby the region continues to be a target of low- to medium-intensity cyber operations. One may argue about whether high resilience can be achieved without more active deterrent measures. On the other hand, it takes two to tango online, too. The higher the active deterrence, the stronger the countering reaction is likely to be. The fear is that this may culminate in a destabilizing cyber arms race.

Higher awareness is needed in order to recognize that cyber operations have strategic aims that go beyond mere snooping and spying. They are effective in spreading mistrust, blackmail and bullying, and in showcasing capabilities and deterrence. They are useful in combination with other political pressuring tools. The spectrum of these combinatorial tools is still relatively restricted. Yet the concern is that the situation may escalate, in which case the level of harm caused by cyber operations will become higher and more intense. One should also note that the level of harm is always realized in hindsight. Dukes and Red October/Turla were only identified a long time after the infections. This suggests that there might already be ongoing campaigns with a higher level of harm that have yet to be detected.

This analysis cannot exclude the possibility of a further escalation in malicious cyber activities. Should this happen, more intense use of cyber tools is to be expected in tandem with other increasingly intense means. If this still unlikely scenario materializes, then the low-intensity cyber operations of today can be seen as a preparatory phase for a far more aggressive challenge directed mainly towards the key functions and stability of the Nordic-Baltic political systems.

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

ISBN 978-951-769-496-4
ISSN 1795-8059
Language editing: Lynn Nikkanen
Cover photo: Max Elman/Wikimedia Commons. Used under Creative Commons license.

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.