



PISM

POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

BULLETIN

No. 25 (875), 24 March 2016 © PISM

Editors: Sławomir Dębski (PISM Director) • Katarzyna Staniewska (Managing Editor)
Jarosław Ćwiek-Karpowicz • Anna Maria Dynier • Dariusz Kałan • Patryk Kugiel
Zuzanna Nowak • Sebastian Płóciennik • Patrycja Sasnal • Marcin Terlikowski

The Swedish Counter-Intelligence Report on Hostile Russian Activities in the Region in a Comparative Context

Marcin Andrzej Piotrowski

The Swedish counter-intelligence service's latest annual assessments highlight the growing interest of Russian intelligence in Sweden's national security issues. Soon after the publication of the unclassified version of the report, a series of cyberattacks on Swedish media took place. The increase in hostile Russian intelligence activities has been seen as connected to a public debate about the prospects for closer relations between Sweden and NATO. The U.S. perception of the Russian threats presented by Sweden's counter-intelligence services does not deviate from public assessments by other Scandinavian countries' assessments. This might suggest that the increased Russian activities are part of some broader strategy concerning Northern Europe.

On 17 March 2016, the Swedish Security Service (Säkerhetspolisen, or SÄPO) published an unclassified version of its annual assessment of intelligence and terrorist threats. The chapter on Russian disinformation and psychological operations stirred public interest and was followed by a series of coordinated and massive cyberattacks (DDoS-style, or "distributed denial of service") on a number of websites in Sweden. A DDoS attack on 19 March resulted in seven of the main Swedish newspapers' internet portals being unavailable.

Russian Threat Estimate by SÄPO. The report prepared by SÄPO is dedicated to intelligence and terrorist threats to Sweden, not military threats. One of its chapters covers the aggressive Russian actions attempting to influence Swedish public opinion. Swedish counterintelligence describes a combined informational and psychological approach by Russia's government that blurs the classic distinction between war and peace. SÄPO's analysts stress that Russia used this approach during its takeover and subsequent annexation of Crimea in 2014. The essence of the tactic is the use of covert actions, disinformation, and sabotage of the decision-making processes of the attacked country. This broad spectrum of techniques of Russia's hybrid warfare is based on the experience within its Main Intelligence Directorate of the KGB (so-called "active measures"), the "Gerasimov doctrine," named after the head of the General Staff of the Russian Armed Forces, and Russia's growing cyberwarfare capabilities.

The SÄPO report also assesses that Russia's civilian intelligence service (SVR) and military intelligence service (GRU) are engaged in aggressive reconnaissance of Swedish civilian and military infrastructure. Their goal is to collect information about weaknesses that would enable further sabotage, disinformation or other attacks on Sweden's state structures. Based on these conclusions in the report, it is clear the service is concerned by the intensifying activities of both classic human intelligence and cyber-espionage employed by Russia. In this context, Swedish media also noted that a previous edition of the SÄPO report had identified 10 SVR and GRU officers among the 37 Russian diplomats accredited in Sweden. The latest edition of the report also emphasises a noted increase in Russian intelligence services' contacts with radical right-wing organisations in Sweden.

SÄPO observed in 2015 the growing influence of Russian media (including RT and Sputnik) on negative perceptions in public opinion in Sweden. Swedish counter-intelligence is thinking that these activities are directed to undermine the credibility of Sweden's political leaders and mainstream media as well as to influence public debates in the country, especially on its foreign and security policy. To reach these goals, Russia is using social media, useful in rapidly spreading false news and pro-

Russian opinions. As an example of this Russian disinformation campaign, SÄPO mentioned a supposed exchange of letters from Sweden's Ministry of Defence and General Prosecutor to the government of Ukraine on the alleged delivery of advanced Swedish weapons (circulated in spring and autumn of 2015), but which were, in fact, forgeries.

Russia's Demonstration of Force. Although Swedish military intelligence (MUST) and its radio-electronic intelligence service (FRA) do not publish similar annual estimates, non-governmental experts are interpreting reoccurring violations of Sweden's airspace by Russian airplanes (multiple times in 2014 alone) as part of the broad spectrum of pressure. The majority of these incidents were a clear show of military force by Russia and coincided with the mobilisation of the Swedish Navy against what it said was an unidentified submarine operating in waters close to Stockholm.

The government of Sweden is also cautious about revealing the source of the latest cyberattacks against the Swedish media sites. However, officials from the Swedish Civil Contingencies Agency (MSB) noticed that these attacks originated from computers outside Sweden and "to the East". MSB, by comparing previous and current data from the DDoS attacks, recognized the latest activity as both coordinated and conducted on a scale not seen so far. This agency (like SÄPO) thinks that the selection and choice of media as cyber-targets were not coincidental. Commentators have noted the effectiveness of the government's servers to resist the attack and MSB's support in protecting them, probably because the anonymous hackers announced their plans a few hours before the attacks began on 19 March. It is clear that the previous serious DDoS attack in October 2012 had shown both the public and private sectors in Sweden were vulnerable. It also should be noted that in Russian official documents and expert publications about cyber-operations, such actions are perceived as an integral part of information warfare. Moreover, Russia already has demonstrated the capability to synchronise cyberattacks with other events, including riots in Estonia (2007) and hybrid warfare campaigns against Georgia (2008) and Ukraine (ongoing since 2014).

Russia's Activities in the Region. The latest report by SÄPO might be compared with similar intelligence services' reports by Finland and the Nordic NATO member-states. In recent years, these countries' security services were focused on preventing and combating terrorist threats, especially from Al Qaeda and the so-called Islamic State, as well as from right- and left-wing radicals. A specific example here is Iceland, a member of NATO but lacking its own armed forces and intelligence services. Finland's security service (SUPO) reports this country is of special interest to Russian intelligence both because of its membership in the EU and its partnership with NATO, and as a target for technological espionage. Obviously, Finland also is an object of Russian shows of force.¹

The Danish Security Service (PET), in its unclassified publications, is indicating high activities in foreign military and technological espionage, noting an equal threat from China and Russia. A more extensive analysis of Russian security policy in the region in 2015 was presented in a report published by the Danish Military Intelligence Service (FE). It assesses Russia as having the capabilities and willingness to use both force and Russian-speaking minorities as instruments of regional policy. According to FE, Russia wants to rebuild influence within the post-Soviet area and to change the strategic situation in the Baltic Sea region. FE estimates that Russia is capable of mobilising its armed forces against the Baltic states within seven days and would attempt to complicate reinforcement by NATO in the region. Denmark's intelligence report also recognizes some risk of hybrid warfare between Russia and NATO, itself, aimed at testing the cohesiveness and credibility of the Alliance. A separate chapter in FE's report is dedicated to the growing military and intelligence activities of Russia in the Arctic region.

An assessment of Russian and Chinese intelligence threats is presented in the latest report by the Norwegian Security Service (PST). This agency estimates that the intentions and capabilities of Russian intelligence might be a particular threat to the national security of Norway. Similar to its Swedish counterpart, PST stresses Russia's high capability for propaganda, disinformation, cyber-espionage, gathering intelligence on military facilities, the energy sector and Norwegian Arctic. PST also noticed constant activities against Russian dissident émigrés in Norway. The Norwegian Military Intelligence (NIS), in its 2015 report, assesses that Norway and NATO should take into consideration in the mid-term the risk that Russia has further capabilities to use civilian and military means and that they may be escalated according to the Kremlin's needs. The NIS also analyses the deeper reforms in the Russian Armed Forces and finds they are more capable of rapid and widespread mobilisation. The NIS report, like the Danish FE, also analyses the possibilities that Russia would use an integrated approach (hybrid warfare) in the Arctic region.

Conclusion. A separate chapter for SÄPO's assessment for 2015 on Russian intelligence and media activities against Sweden indicates the level of Russian efforts to influence the latter's security policy and is seen as dangerous to Swedish interests. It should not be excluded that the latest cyberattacks on Swedish media that discussed the counter-intelligence report also may have been Russia's retaliation for the assessment's frankness and explicitness. These cyberattacks also may have served as a test of Russia's offensive capabilities and Sweden's defence of its administration and private sector networks. Comparing the analyses of SÄPO with other unclassified intelligence reports from the region shows a picture of the implementation of a comprehensive Russian strategy towards the area of the Baltic Sea, Scandinavia and the Arctic, in which it combines intelligence-gathering, lobbying, disinformation and military means to meet its aims. This strategy might be calculated to influence the public debates in Sweden and Finland on the prospects of their membership in NATO while frightening both societies with the threat of "unpredictable consequences" if their countries join the Alliance. The long-term goal of these Russian activities in Northern Europe might also be to weaken cohesion in NATO, itself, and to generate disputes among the Allies about their future relations as well as military cooperation with Sweden and Finland.

¹ For more, see: W. Lorenz, "Finland Gets a Foot in NATO's Door," *PISM Bulletin*, no. 93 (668), 30 June 2014.