Prepared Statement of Janis Sarts, Director of
NATO Strategic Communications Centre of Excellence

on

Russian Interference in European Elections
United States Senate Select Committee on Intelligence

June 28, 2017

Thank you, Mr. Chairman, Mr. Vice Chairman, for the opportunity to share my views on Kremlin influence operations in Europe, as well as present some ideas on how to counter these risks and develop social resilience to disinformation attacks.

Background

Before exploring this subject, I would like to tell you about the work done at the NATO Strategic Communications Centre of Excellence. The Centre is a NATO accredited international institution created by 11 countries to assist NATO and its allied governments in the development of strategic communications capacities. The Centre is not part of the NATO command structure and is guided by the 11 nations sponsoring the Centre. Thus any views expressed by me as Director are the views of the Centre and do not represent NATO's position as agreed by its 29 member nations.

Our work is centered on researching the phenomenon of information warfare through case studies, lessons learned, and experimentation. Over the past two years we have produced 18 studies that examine different angles of Russian information operations. Based on this research we develop methodologies and techniques that can be employed by NATO and its allies to counter such activities.

The use of influence operations has a long history. During the Cold War the USSR frequently referred to them as "active measures". Thanks to the documents and personal stories that became available during the 1990s, we can now verify that the KGB was primarily responsible for implementing such active measures. It has only been in the last decade that these methodologies have come to be prioritized in Kremlin. After a series of recent failures, including faulty information management during Russia's incursion into Georgia in 2008 and the protests in 2011 that followed V. Putin's bid for a third presidential term, the active measures developed by the KGB have returned to the forefront.

In early 2013 Russian Army General Valeriy Gerasimov described the elements of a new type of conflict where information confrontation is the central element central to all six phases of conflict evolution as defined by the Russian army. In a statement to the Russian State Duma in 2017, Russian Defense Minister Shoigu confirmed that Russia has established information warfare troops within the state security structure.

Tools

The tools Kremlin now uses in its influence operations are a combination of the tools used by the KGB during the Cold War and new elements that exploit our growing technological dependencies. Traditional media outlets are still extensively used to promote Kremlin

propaganda within the context of larger influence operations. It is worth noting that the overwhelming majority of Russian news media, reporting within Russia and abroad, are under the direct or indirect control of the Kremlin.

Traditional influence techniques are still in use today. There are many recent examples of news manipulation in the Russian media. During the peak of the European refugee crisis in May 2016, Russia's Channel 24 interviewed locals in France and later reported on these interviews. However, the so-called translations directly contradicted what was actually said in the interviews. In another example, a French school that had been closed for five years was opened to accommodate the refugees; the Russian media reported that the refugees had violently taken over the school. Interviewed French people said they felt safe with the influx of refugees, but the Russian media reported them as saying they felt very frightened.

Today technological developments have vastly increased the reach of information operations. Current online possibilities enable fast, cheap, and geographically unlimited opportunities to spread information. In fact, cyberspace has become a parallel platform for information activities. Actions in virtual space can be used to influence developments in physical space and vice-versa. For example, a well-known information operation, known as the Lisa Case, took place in January of 2016. Many Germans of Russian origin and right-wing extremists went out into streets in Germany to protest the alleged rape of a young Russian girl in response to reports that the alleged perpetrator was a refugee. In fact, there was no rape, but fake information had been convincingly disseminated via social media.

The newest additions to this list include robotic tools such as bots, trolls, and "like-machines". Robotic trolling is coordinated activity by fake accounts in digital media. We can say that at least 8%[1] of Twitter accounts and 5-11%[2] of Facebook accounts are actually bot accounts. The activity of the bots can vary depending on the effect the manager of a bot or troll network wants to achieve with regard to a particular issue. As with any information activity, the goal of robotic trolling is not to persuade but to confuse. Nevertheless, some social media users may perceive emotional and fact-free comments as trustworthy, especially when they are often repeated and appeal to the convictions of those individuals.

Most of these activities seek to exploit preexisting vulnerabilities such as prejudice against minorities, social inequality, migration and corruption. They disrupt normal political processes and to establish an "information fog" that undermines the ability of societies to establish a factual reality.

Cases

Increasingly Kremlin has learned that election periods provide excellent opportunities to use their tools of influence. Properly deployed, these tools have the potential to directly affect the political landscape of the country in question, and, consequently, policies important to Russian interests. Although some cases have been recorded before 2008, Kremlin' s meddling in elections intensified after Russia's incursion into Georgia and peaked after anti-Russia sanctions were imposed following annexation of Crimea. It appears that election meddling is

[1] Twitter Has Stopped Updating Its Public Tally Of Bots, William Alden, BuzzFeed, 10 November 2015. https://www.buzzfeed.com/williamalden/twitter-has-stopped-updating-its-public-tally-of-bots

[2] Facebook estimates that between 5.5% and 11.2% of accounts are fake, Emil Protalinski, The Next Web, http://thenextweb.com/facebook/2014/02/03/facebook-estimates-5-5-11-2-accounts-fake/

done to either promote candidates friendly to Kremlin or those trying to undermine the EU and NATO and hurt the candidates Kremlin perceives as undesirable.

Election meddling is primarily conducted through:

- Financing pro-Russian candidates and political parties and offering the Kremlin media as platform (Estonian EP elections 2009, French Presidential elections 2017)
- Cyber-attacks against candidates Russia perceives as unfriendly
- Malicious disinformation using social media bots and Kremlin-aligned fringe media outlets

There have been numerous cases in Europe where local authorities have publicly stated that Russia has tried to influence election outcomes.

In 2009 in Estonia: KAPO, the Estonian special service, stated that Russian special services were trying to influence the 2009 European Parliamentary election in Estonia in a way that would lead to the election of a Kremlin-friendly to the European Parliament.

In 2014 in Ukraine: "Fancy Bear Malware" was used to infect the servers at Ukraine's central election commission ahead of the election to declare the Right Sector candidate Dmytro Yarosh as the winner.

In 2015 in Germany: The Russian hacker group APT28 hacked into the German Bundestag, which caused fear that the stolen information could be used to influence the vote in 2017. Hans-Georg Maassen, head of the BfV agency responsible for cyber security said "Our counterpart [in Russia] is trying to generate information that can be used for disinformation or for influence operations".

In 2016 in Montenegro: Montenegro's prosecutors accused Moscow of orchestrating a coup attempt during Montenegro's October 16 election in a bid to stop the country from joining NATO. "So far we have had evidence that Russian nationalist structures were behind [the plot], but now also that Russian state bodies were involved at a certain level," said prosecutor Milivoje Katnic, according to AFP.

In Norway in 2017: Russia-linked hackers attacked government ministries and an anti-Russian political party.

In the Netherlands in 2017: Domestic intelligence officials reported that foreign countries, notably Russia, have tried hundreds of times in recent months to penetrate the computers of government agencies.

The most recent case was during the presidential elections in France: The Kremlin's strategy was to support Marine Le Pen, and do anything to discredit her opponents. This included providing her party, the National Front, with Russian financial backing. In 2014 the National Front received € 9.4 million paid out by the First Czech-Russian Bank and signed an additional loan application with the Russian NKB bank on 15 June 2016. The last loan of 3 million euros was "intended to finance the French election campaign". In the run up to the elections in March 2017 there was a surprise meeting between Marine Le Pen and Vladimir Putin that received broad coverage by Russian media, including the French outlets of RT and Sputnik.

Sputnik and RT published rumors of the "double life" of Emmanuel Macron, saying that he is supported by a "very rich gay lobby". Since its launch, Macron's party *En marche!* has

undergone more than 2500 intrusion attempts, including 907 from the Ukraine. These cyber-attacks "suddenly increased" in January, when the election polls showed increasing popular support of Macron.

The Atlantic Council's Digital Forensic Research Lab has tracked down networks of bots involved in promoting the candidates favored by Russia in various elections including Geert Wilders in the Dutch general election campaign and Marine Le Pen in the French Presidential election campaign. Although their connection to the Kremlin cannot be confirmed, the narrative spread by the bots was identical to that of the Kremlin-funded media, and synergies between two were frequent and consistent.

Response

First turning point for NATO and European NATO allies was the annexation of Crimea by Russia and the start of the conflict in Eastern Ukraine. NATO developed strategy for countering hybrid warfare, NATO nations established Strategic Communications Centre of Excellence in 2014.

In order to confront Russian information confrontation NATO is applying 2 different approaches. First of all NATO invests extra time and effort to inform and to explain its home audience as well as outside audiences about NATO goals and actions. NATO narrative of collective defense and security should be circulated and showed by NATO's deeds first of all by NATO itself. And that is what NATO does. Subsequent monitoring and assessment of how your narrative resonates with expectations and perceptions of your target audiences are important for further strategic communication of NATO.

Other track which NATO undertakes is an assessment of hostile information activities against NATO. Current NATO operations have additional focus on information environment assessment of the operation theater. That includes identification, tracking, monitoring and analyzing of hostile information activities. It is a new capability which is being developed via several tracks simultaneously and includes current operations, concept development of information environment assessment tools and processes and development of the new NATO capability. Also the newest NATO mission –"Enhanced Forward Presence" of allied troops in Estonia, Latvia, Lithuania and Poland is faced with the increased amounts of false information, starting with allegedly raped teenage girl by German soldiers' case in Lithuania, to Canada sending "gay" battalion to Latvia. NATO has put in place mechanisms to address and counter these information attacks effectively.

European governments have also started to increasingly address the problem of Russian disinformation and influence operations. I see three generic tracks that are being pursued: organizational, capability development and work with the society.

Typically foreign influence operations are handled by the special services within the countries, but increased public nature of these activities have limited the effectiveness of the tools that can be deployed by these institutions to counter the challenge. More and more the response has also to be public and immediate. Increasingly governments choose to give the principal coordination responsibility to the central element of executive power – prime minister. In countries such as Finland, Estonia, Latvia and Poland central government body has people tasked with coordination and implementing the response to these threats. In other countries Sweden, Czech Republic, Lithuania agencies are given new responsibilities and resources in this area.

Secondly, more resources are being devoted to develop capabilities in two essential response areas- cyber defence and strategic communications. In large majority of European nations there is a growing trend to invest more in one or both of these elements. Germany recently created a new Cyber Command as part of their military system, countries are also increasingly investing in their military and nonmilitary strategic communications capabilities including new information flow monitoring systems.

Thirdly, as most of the influence attacks aim at changing society's perceptions and thus behavior models, governments increasingly work with civic society, to build necessary resilience. Increased funding for investigative journalism, and objective journalism, increased media literacy, work with fact checking groups are just some of the lines of effort taken by European nations. As the result, in some countries there is increased activity by citizens to engage and counter disinformation, the most prominent being so called " Elves" in Lithuania and Latvia- groups of civic activists that fight ' Trolls " and their messages in online environment.

Recommendations

Raising society's awareness. As has been described before, society and its perceptions are the main targets of the contemporary influence operations. Accordingly, one of the key resilience mechanisms, our research shows, is awareness of the society of being targeted by third party malicious actors to affect their election behavior. We have seen resilience levels raise instantly as society recognizes being targeted by outside actor.

To accomplish it working with the media is one of the key parameters. Not only it is the key tool to uncover the potential fakes and strategies to undermine cohesion of social processes, media are usually manipulated by Kremlin, by understanding their instinctive reactions to "sensational" material , as tools in the given influence operation. I believe, France presidential election second round and the reaction of the main French media in the run-up to the electoral vote is one of the good examples of media response through understanding how they are used in the attempts to impact last minute election choices.

Situational awareness. In the modern information environment the old monitoring techniques are far from sufficient. If society is under outside influence attack, it has to use the tools that enable the situational awareness of the information space that correspond to that what we require of more traditional battle space. What kind of information bubbles (eco cambers) society consists of? Do we see foreign influence in these bubbles? What kind of narratives, hashtags, in support of which foreign actors are the robotic networks pushing? To what end? Is our citizens' data being sucked out by outside actors? These are just some questions that in the new information environment we have to be able to answer to keep our enemies at bay.

Cyber defence. In the western methodology we tend to see and approach cyber world as that of algorithms, networks, data clouds and machines. We forget that increasing number of the cyber-attacks through the technical world attack human consciousness either through typical phishing attack or more complex influence operation. Still it is and will increasingly be important to build cyber resilience both within technical contexts, but increasingly within human context.

Working with the technology companies. As I have argued before, most of the Kremlin influence techniques are comparatively old, what has enabled their new efficiency is the different information environment where the confrontation takes place. The new technology

platforms are the place where most of these methods are most efficient. I would argue, that it is not the technologies fault, but mostly how they interact with human mind. We should increasingly work with the tech companies to counter the disinformation trend. We have to see the ways we can use the new technologies to help and educate our societies to distinguish fact from fiction, normal social debate from foreign influence, a real human from a robotic program used to push the subject.

Finally Mr Chairman, Mr Vice Chairman. The influence operations Kremlin is pursuing are based on old soviet techniques combined with clever use of our technologies and increasingly of our marketing knowhow. I see no reason why we should be losing. It is about acknowledging the problem, resourcing solutions and using that is best in our societies (free speech, civic engagement, innovation) to win it for our future.