

INSS Insight No. 1031, March 8, 2018

Russian Intervention in the US Presidential Elections:
The New Threat of Cognitive Subversion
Yotam Rosner and David Siman-Tov

The indictment filed by the United States Justice Department on February 16, 2018 against 13 Russian citizens and three Russian companies is a document without precedent. The evidence indicates massive and systematic involvement by Russian elements in the internal US public debate in an attempt to promote the candidacy of Donald Trump for the US presidency, amounting to intervention in the country's political system. Following the filing of the indictment, President Trump admitted this involvement for the first time. While Russian Foreign Minister Sergey Lavrov has dismissed the accusations, it is now clear that democratic governments in the West are beginning to understand that they must prepare for what looks like a significant strategic threat to their stability: manipulation of the public discourse by external elements seeking to undermine social unity or damage public trust in the political system. This phenomenon, namely the link between psychological warfare methods and technological infrastructures, enabling intervention in the "consciousness" of another country, could be called "cognitive subversion."

The details in the US indictment reveal a sophisticated conspiracy, including organizations and companies that received funding estimated in the millions of dollars starting in 2014, in order to generate a broad media campaign and influence the political discourse. The actions of the accused were based mainly on the use of social media platforms to spread content that promoted the candidacy of Trump and other non-establishment figures, including Bernie Sanders, Ted Cruz, and Marco Rubio in swing states, such as Florida and Pennsylvania. The messages were not limited to support for Trump and the other candidates, but included tactics such as masquerading as Muslim supporters of Hillary Clinton and purchasing advertising space on Facebook, which contained messages such as "Support Hillary. Save American Muslims." The purpose was to create a link between political Islam and Clinton.

This cognitive subversion by Russia extends beyond the US presidential elections. Intelligence agencies in the United States, Britain, and Spain that investigated the matter found evidence of similar involvement by organizations linked to Russia in some 19 states. The findings show that for years Russia has operated a huge network of talkback writers, hackers, and narrative shapers, so as to formulate messages that will reverberate

in the public discourse of democratic countries and promote specific goals: splitting the Western camp, supporting movements and candidates with a separatist-nationalist agenda, and above all, undermining the public's faith in the democratic system and institutions. The purpose of the intervention was not necessarily to promote a particular candidate, but rather to paralyze the political system with internal rifts, making it hard for decision makers to take effective action. The guiding logic was that a polarized political system is a convenient rival, whoever is at the helm.

The most significant space in Russia's campaign to influence the system is provided by the huge social media platforms, above all Facebook, Twitter and YouTube, alongside media identified with the Kremlin, such as the Russia Today (RT) television station, where messages are disseminated. Messages are spread using two main tools: trolls (some based on identity theft) and bots (robots). Trolls are paid talkback writers, while bots are software programs that can write thousands of posts or responses on social networks. Together these tools can distribute a vast quantity of messages to arouse conflict, hatred, and violence on social media, in discussion groups, and in responses to press articles. There is also information about advertising space purchased for messages supporting the Russian position and about the segmentation of messages for specific target audiences to increase their effectiveness.

It is very important to distinguish between legitimate messages that emerge within a country's political system and civil society, and illegitimate messages, based on fraud. There are two types of fraud: distorting facts and fabricating news stories; and falsifying and stealing local identities in order to be perceived as an authentic voice, to reinforce the effect of the message on its target audience.

Cognitive subversion exploits one of the basic principles of democracy – freedom of speech. The belief that freedom of speech is the foundation of a democratic society has eroded in recent years, particularly in light of the development of social networks that have become a significant source of news information and political discussion. In an ideal situation, social networks enable people to express themselves and increase their participation in public debate. At the same time, they enable opportunistic elements to spread "fake news" (disinformation), and silence positive public debate by mudslinging and deceiving the public. Although public representatives also intervene in the public discourse and engage in manipulations by spreading divisive and opportunistic messages, in these cases the source of the statements is identified and so their influence is limited. This is not the case with inflammatory messages from foreign sources, disguised as authentic local voices.

In democratic countries, the abuse of social networks has been challenged by increased regulation, legislation, involvement of the security services, and fact-finding teams (in governments and in social media companies), and by the involvement of civil society. These moves acknowledge the awareness that foreign elements can make strategic gains if they are able to shape the public discourse, particularly in societies dealing with severe social rifts, with their own potential to create political shocks.

This challenge is also relevant to Israel and requires it to take action. Demographic and political processes in Israel in recent decades have led to severe social, ethnic, and political polarization. This multi-faceted polarization, referred to by President Reuven Rivlin in the "tribes speech" he gave in 2015, is highly significant for Israel's national resilience. Inter alia it can be exploited by hostile elements trying to widen the rifts and thus reduce the possibility of establishing a legitimate national leadership, with the ability and the mandate to make decisions.

Accordingly, Israel requires a national cognitive strategy, with the emphasis on the defensive aspect, to be expressed in legislation, budgets, and definition of areas of responsibility for new or existing entities. In addition, civil society must be harnessed to deal with this new threat. These measures should be taken while balancing the need to protect public discourse and the need to preserve freedom of expression and individual liberties.

In recent years there has – rightly – been growing awareness in Israel of cyber threats to critical infrastructures and the civil economy. In response, the government established the National Cyber Directorate and took steps to raise awareness of this danger. Without playing down the magnitude of cyber threats to the function of the economy and infrastructures in war and in normal times, it is important to point out the paradox, whereby those who wish to manipulate the political discourse, in Israel or anywhere else, actually need essential infrastructures (electricity, internet suppliers) to function properly and so will not try to disrupt them.