INSS The Institute for National Security Studies
Strategic, Innovative, Policy-Oriented Research

INSS Insight No. 858, September 26, 2016

The Superpower Cyber War and the US Elections

Gabi Siboni and David Siman-Tov

In late July 2016, about the time of the opening of the Democratic National Convention (DNC), the WikiLeaks website publicized embarrassing emails from the accounts of senior party staffers. The hackers gained full access to the DNC network used by the election staff, including emails, memos, and research performed for Democrats running for Congress. The widespread belief was that the hackers were Russian-based, and the operating assumption of US law enforcement agencies was that Russian hackers had broken into the computer network serving the DNC as part of a cyberattack aimed at Democratic Party institutions. In an interview with Fox News, Democratic candidate Hillary Clinton accused Russia’s espionage services of the break-in and the leaking of the emails. She noted that there were reliable reports pointing to Russian involvement that intended to disrupt the electoral process. The National Security Unit within the US Department of Justice is investigating the extent to which these cyberattacks indicate significant Russian involvement in the US presidential race.

In a similar vein, Senate Democratic Minority Leader Harry Reid issued a warning about possible attempts by Russian attackers to rig the presidential election results. In late August, he asked the FBI to probe the possibility that over the previous weeks foreign hackers had already infiltrated the databases of the Central Election Committee in Illinois and tried to penetrate similar databases in Arizona. So far, officials estimate that the hacks have resulted in the theft of some 200,000 voter registration entries. The concerns center on the possibility that hackers have erased or might erase the databases storing the election registries or might damage the reliability of the election results in some other way. In a letter to the FBI, Reid wrote that “I have recently become concerned that the threat of the Russian government tampering in our presidential election is more extensive that widely known and may include the intent to falsify official election results.” According to Reid, in recent briefings senior US intelligence officials warned that Russian President Vladimir Putin is interested in undermining the electoral process. Given these concerns, US Secretary of Homeland Security Jeh Johnson offered election committee representatives the help of the federal government in securing their computer systems.

Immediately after the report of the attack on the DNC, Kaspersky Ltd. exposed an advanced and widespread Russian cyber espionage scheme called Project Sayron. Officials estimate that this operation has been active in Russia for several years, but the timing of its exposure is no coincidence, and shows that the United States too operates in Russian cyberspace. For their part, the Russians attribute the attack to the United States, and the FSB, Russia's internal security agency, said that the same attack is also targeting security institutions. Presumably the publication of the break-in and theft of secret NSA malware is linked to this scuffle between the United States and Russia. This theory was reinforced after Edward Snowden, who was granted asylum in Russia and may even be a Russian operative, suggested that Russia was behind the break-in.

The escalation in cyberspace between Russia and the United States comes on the heels of offensive cyber missions launched by Russia in Syria and Ukraine, and apparently other East European nations as well. In all probability, the purpose of the attacks is to display Russia's might and technological prowess, primarily in order to create deterrence. Presumably the attacks on the United States were similarly motivated, and designed to exploit the presidential elections to showcase Russia's capabilities with maximal exposure. Indeed, Russian involvement in the elections process sends a strategic message of the highest importance. The attacks on the United States are thus a new twist in cyber aggression, first of all insofar as the electoral system in a democracy represents the nation's bedrock infrastructure, and therefore needs supreme protection. There are many ways in which cyber activity can cause damage, from online election disruptions to falsification of the actual results. In a second circle, the falsification of public opinion polls or the manipulation of announcement to the voting public are liable to cause systemic disruption of the elections as per the attacker's own interests, be the attacker within the country, from a rival political party, or from a foreign nation.

Voices in the United States have been urging the administration to make it clear to Moscow that a Russian attack on the democratic process will be met with an appropriate response that may not necessarily be limited to cyberspace. These events are a reminder of the urgent need for developing international norms to reduce the possibility of cyberattacks on electoral processes. In the early 2000s, Israel was a pioneer in this realm, when it defined the need for protecting critical infrastructures to ensure state functioning, including a state's electricity, energy, and communications systems. Later, other installations were added to the list, such as the banking system and e-commerce. The electoral system is a critical infrastructure of a new type: it is the soft underbelly found only in democracies. It can be attacked in a range of ways, from pinpoint damage at particular polling stations to systemic disruption liable to erode the voters' trust in their elected representatives and faith in the democratic system as a whole. The disruption of the voting system could focus on election day, the primary weakness, but could also occur over the months preceding the election: results of primaries might be manipulated, public opinion polls falsified, and psychological warfare waged in the media. The events of this past month demonstrate Russia's audacity and the United States' mild response, and we probably haven't heard the last word of this round (especially as many ascribe to Russia an interest is seeing the Republican candidate in the White House).

In addition to the construction of covert offensive capabilities in cyberspace by some nations, the intentional revelation of cyberspace assets at a particular time has become a relevant issue. In other words, if in the past cyber attacks were aimed primarily at intelligence gathering and espionage, or if they sought to damage critical processes and systems performance, there is now a phenomenon whereby attackers accrue assets and activate them publicly when the attackers feel it will best further their interests, even at the possible cost of losing those assets; hence the very tight connection between cyber warfare and psychological warfare. The Russian attackers – or at least the attackers with some link to Russia – are clearly not worried about losing their cyber assets as long as they can promote their interests. Note that a proactive exposure of cyber assets is opposed to the nature of Western intelligence communities, which generally prefer to operate covertly.

Beyond the connection to conventional wars, cyber warfare is relevant to routine relations between world powers. More specifically, we are witnessing a new kind of cyber war that proceeds without the public's awareness, and in which it is not always clear who is doing what and why. Apparently as a result of tensions between Russia and the US, and perhaps other states as well, a cyberwar is already underway that beyond the ongoing activities of intelligence gathering and espionage, includes psychological warfare and damage to democratic processes, in this case, in the United States. The effect of damage to the democratic process, perhaps by means of tendentious exposure of materials liable to affect the voting patterns of target groups, for example, is an act with very broad strategic implications.

State systems are traditionally mobilized in times of emergency and kinetic warfare. However, the recent cyber events have occurred in routine times, and Western states have yet to internalize that the routine itself is a guise for a cyber campaign that has widespread strategic implications. Accordingly, the recent cyber-related events challenge the traditional political definitions of routine, emergency, and war, and in turn demand appropriate conceptual and organizational preparations.

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
INCORPORATING THE JAFFEE CENTER FOR STRATEGIC STUDIES
TEL AVIV UNIVERSITY
אוניברסיטת תל-אביב