BESA PERSPECTIVES
THE BEGIN-SADAT CENTER FOR STRATEGIC STUDIES

Cybersecurity: Recommendations for President Trump, Implications for Israel

by Col. (res.) Shay Shabtai

BESA Center Perspectives Paper No. 405, February 1, 2017

EXECUTIVE SUMMARY: Two reports on cybersecurity – one commissioned by President Obama and the other by CSIS – have been placed on the desk of President Trump. They are different in their approach: one promotes an evolutionary policy based on procedural and "soft" tools, and the other espouses an activist approach domestically and a more combative one regarding foreign opponents. Both contain recommendations that may be relevant to Israel, including a national program to strengthen identity authentication mechanisms, a nationwide "protective umbrella," a national awareness campaign, and the transfer of government infrastructure to external cloud services. Israeli hi-tech industry could also be incorporated into the programs suggested in the reports, should they materialize.

Cybersecurity has garnered significant headlines in the US in recent months, and was an issue during the election campaign and the administration transition process. In his last weeks in office, President Obama took punitive steps against Russia after the intelligence community determined that the latter had acted to obstruct and impact the American electoral process.[1] After becoming privy to the classified information about Russian activities, then President-elect Trump appointed Rudy Giuliani, who heads a security (including in cyber) consulting firm, as an informal advisor on cybersecurity.[2]

Two reports have landed on the president's desk dealing with US cybersecurity policy. One was submitted to President Obama on December 1,

[1] DNI, Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution, 6 January 2017.
[2] Abby Phillip, Trump names Rudy Giuliani as cybersecurity adviser, *Washington Post*, 12 January 2017.

2016 by a nonpartisan commission he appointed.[3] It was written by a team led by Tom Donilon, the former National Security Advisor, and General Keith Alexander, the former Director of the NSA, with the assistance of administration experts, especially from NIST.[4] The other report was prepared and published in January 2017 by the Center for Strategic & International Studies (CSIS) for the President-elect[5] by a taskforce led by Democratic Senator Sheldon Whitehouse.

What can we learn from these reports that might be relevant for Israel?

The reports' starting-point is the assumption that the digital world, which has become an essential element for human conduct as well as for the global and American economies, is based on vulnerable technologies. Among the reasons for this is the disparity between the profits from digitization, which reach the trillions of dollars, versus the damage incurred by cyberattacks, which stands at the tens of billions. Consequently, security needs are pushed back in the face of the clear priority given to speed of development and market penetration; creation of a flexible work environment for employees, including remote working and use of personal equipment in the workplace (BYOD, or Bring Your Own Device); increasing connectivity and reliance on chain of supply; and implementation of complex technologies that are inherently more vulnerable.

In an environment with those characteristics, business organizations consider cybersecurity a side issue. Some disregard even the most elementary steps required. The attackers have a distinct advantage because all they need to do is locate a single weakness. These are sophisticated and up-to-date entities that adopt the most advanced technologies in parallel to, and at times even a step ahead of, cybersecurity defenders.

Government bodies, which are also increasingly dependent on information technology, suffer from inherent failings: outdated information infrastructure; procurement processes that are not adapted to the digital age; non-competitiveness in recruiting high-quality personnel compared to the private sector; and difficulties in planning, resource allocation, and implementation of long-term trends, in part because of the complexity of budgetary processes.

---

[3] Commission on Enhancing National Cybersecurity - Report on Securing and Growing the Digital Economy, 1 December 2016.

[4] The National Institute of Standards and Technology.

[5] A Report of the CSIS Cyber Policy Task Force - From Awareness to Action - A Cybersecurity Agenda for the 45th President , January 2017.

This situation is exploited by cyber-attackers for three purposes: weakening of critical infrastructure and processes, espionage and information theft, and crime. The US is facing significant losses from attacks on critical infrastructure and processes of the state by state actors (the statement by the intelligence community heads to the Senate mentions Russia, China, North Korea, and Iran)[6] and terrorist elements; defense and economic espionage, which results in the loss of intellectual property and a reduced military qualitative edge; and cyber-crime. These cost the US a collective estimated annual $100 billion, and $450-600 billion globally.

As to solutions, the reports are divided. The report submitted to President Obama, but directed at President Trump, is premised on the continuity of the current situation and on development based on procedural and "soft" tools: incentives, standards, awareness, research and development, professional training, and management responsibility. This is in pursuit of four goals: protection of privacy, safety and security, the development of the digital world, and the strengthening of partnerships. The overall object is to improve current cyber-protection and develop a forward-looking response.

The CSIS report, on the other hand, is characterized by a more activist and combative approach. It calls for a fundamental change in existing cybersecurity policy. It establishes that reliance on the private sector and market incentives, such as insurance, will advance cybersecurity solutions too slowly (if it does so at all) in relation to the developing threat. The report's recommendations expose the inadequacy of government bureaucracy, which is mired in outdated "clichés" that cannot be realized. These include information-sharing mechanisms; public-private partnerships; efforts to strengthen "innovation"; grand national initiatives; voluntary international norms that are disregarded by attackers; and the idea of "active defense." Against all these, the report sets two principles: raise the consequences for foreign actors, and incentivize domestic actors to provide better cybersecurity.

A number of practical recommendations in these reports may be highly relevant both for Israel's cybersecurity policy and for Israeli hi-tech industrial activity in the US:

1. **An approach that exacts costs from opponents**: a proactive approach that involves sanctions and prosecution of foreign entity attackers (as opposed to deterrence, which is problematic in the context of cyber); an assertive response to cyber-crime; an exertion of pressure on states to deal harshly with attackers operating from their territory.

[6] James R Clapper, Marcel Lettre and Admiral Michael S. Rogers, Joint Statement for the Record to the Senate Armed Services Committee - Foreign Cyber Threats to the United States, 5 January 2017.

2. **Cybersecurity as a Homeland security issue and responsibility**: Preference should be given to the Department of Homeland Security (DHS) over the NSA and Cyber Command. As a result, a "National Cybersecurity Agency" should be established under the DHS and cybersecurity should be added to the responsibilities of the National Guard. In parallel, the Cyber Threat Information Integration Center (CTIIC), established under the Director of National Intelligence (DNI), needs an expanded role along the lines of the National Counterterrorism Center (NCTC).

3. **Creating a nationwide "protective umbrella" for all computing networks:** In cooperation with the business sector, the government should build broad protection for computers, computing networks, wireless networks, and widely used services, such as GPS, to spare the individual end-user constant concern over cybersecurity. The focus of this broad protection should be on small and medium businesses that constitute a key component of the national economy.

4. **Creating consumer awareness**: A national culture of cybersecurity should be developed under this "umbrella." This would be created through public service campaigns and awareness mechanisms, including a security-standard rating of products and development of mandatory training programs for specific groups like CEOs. The content of these campaigns and their related professional procedures can also be used in Israel.

5. **An extensive response for the developing networks of sensors and local computing systems** (called "the Internet of Things," or IoT). These should be based on high standards of protection ("Security by Default"), including strong identification management mechanisms. The backdrop to this is an understanding of the interdependent connectivity between the sensitive networks of critical, national infrastructure and computing of physical systems (Operational Technology), networks of chains of supply and mass-use products such as mobile phones and IoT, which require a high level of protection as well.

6. **A national program to strengthen identity authentication mechanisms**: The goal is to eliminate significant infiltration into systems by means of identity mechanisms by 2021. Within this framework, the government will assist in constructing solid identity authentication mechanisms to be used by the civil sector, strengthening

identity management among service providers, and leading an evaluation process called Privacy Impact Assessment, or PIA.

7. **Strengthening government computing**: This would entail IT consolidation of government agencies and storage in external cloud services – an environment with higher-level security mechanisms than among existing agencies' servers. In addition, it involves a government plan to reduce the number of software vulnerabilities, among others, through regularizing programs rewarding the disclosure of vulnerabilities ("Bug Bounty").

8. **Unlimited use of encryption**: The encryption of information infrastructure to prevent attack should take precedence over the desire to keep these technologies out of the reach of terrorists and criminals. It is better to distribute encryption capabilities and create stronger cybersecurity while managing the risk of its use by negative factors.

9. **Accelerating the training of cybersecurity professionals**: The world will need an additional 1.5 million cybersecurity professionals by 2020. To close the gap in the US, 100,000 professionals need to be trained and another 50,000 placed in apprenticeship programs by that year. In parallel, it is suggested to bring 25,000 cybersecurity professionals into the US from abroad, as well as accelerating the development of related curricula to be taught from primary school upwards (though this is long-term planning).

10. **Research and development of technological solutions**: Federal investment of US$4 billion funneled over ten years through the Director of the Office of Science and Technology Policy (OSTP) and other R&D agencies such as DARPA.

Col. (res.) Shay Shabtai has over twenty years' experience as a field expert on the Middle East, Israel's defense strategy, and military strategic planning. He serves as a strategic consultant for the cybersecurity consultancy firm Konfidas (www.konfidas.com). He is a lecturer in the Military, Security and Intelligence Program at Bar-Ilan University's Department of Political Science, and a PhD candidate, specializing in the impact of intelligence on the national security perception. *The author wishes to thank his colleagues at Konfidas for ideas included in this piece.*

BESA Center Perspectives Papers are published through the generosity of the Greg Rosshandler Family