National Cyber Security in Israel

Yigal Unna

The challenges that the State of Israel faces in the field of cyber technology are affected by sweeping international social, cultural, and technological processes, far more than in other fields. We can identify two challenges or trends that influence cyberspace and are also shaped by it. The first trend—a leading global development—is the challenge of data. Information is the most significant resource of the past fifteen years and seemingly of the coming decades. The main issues relating to this challenge are how to transfer, move, store, and manage data, and how to maximize its benefit. Fifteen years ago, the world's biggest companies were those considered to have the highest value: energy, gas, and oil companies; today, they are information companies. The race for power through information and its control is expected to continue and even intensify in the future.

The second trend is the technological challenge or the "internet of everything," which—beyond the "Internet of Things—is connected to living human tissues for the purpose of monitoring and healing diseases and more. Israel is handling this challenge relatively well compared to the international arena. Israel could still invest more in the field, however, as formulated by the new Technological Intelligence Systems Initiative, pursuant to a directive by the Prime Minister, for identifying the main technologies that Israel should focus on in the near future, namely artificial intelligence, quantum computing, and other data technologies. This is in order to better prepare for the future as a national economic and social power.

Yigal Unna is the director general of the Israel National Cyber Directorate. This article is based on his speech given on October 24, 2018 at the conference held by INSS in cooperation with the Academic Center of Law and Science in Hod HaSharon to commemorate the publishing of the memorandum "Regulation in Cyberspace," by Prof. Col. (res.) Gabi Siboni and Ido Sivan-Sevilla.

The definitions of the terms "cyber," "cyber warfare," and "cyberspace" are constantly changing and being updated. The Israel National Cyber Directorate in the Prime Minister's Office works according to a broad definition that will always remain relevant in order to ensure that Israel has the broadest possible protection against all threats to information and communications technologies (ICTs) as well as additional threat profiles. In this respect, it is worth noting the series of state-level attacks that have taken place in recent years, such as the ongoing series of various attacks on Ukraine since 2014. None of these attacks has led to the collapse of the Ukrainian State, but they have completely disrupted its economy and undermined the public's confidence in the government and its ability to govern.

An assessment of the development of cyberspace and cyberattacks shows that in the beginning, these attacks were aimed at espionage and obtaining information and that they are taking place at greater volume and intensity. Over time it has become clear that by penetrating a computer system, it is possible not only to extract information from it, use it to disrupt critical processes, and even cause physical harm and death, but also to cause psychological harm and have a negative impact—again, all via cyber technology; i.e., by penetrating or breaking into an information system without permission and gaining access to it.

A recent example of psychological harm can be found in the attempts to disrupt the US elections in 2016 which, according to US claims, were under cyberattack. This incident clearly indicates the psychological impact that a cyberattack can have and its success in shaking up an entire election. Additional examples include penetrating the private email accounts of American senators and of a senior official in the US administration, not for the purpose of espionage or inflicting damage, but rather for collecting material that could be leaked at the right time and place in order to cause chaos and undermine the American public's confidence in its democratic and political system.

A well-known example of a psychological attack in the economic sphere occurred two weeks after the terrorist attack at the Boston Marathon in 2013. A tweet was posted on the Twitter account of the Associated Press, stating "Explosion at the White House, President Obama injured." The incident immediately affected the US stock market. In this case, however, the attacker was not sophisticated enough, as it took the news agency only seven minutes

to understand that someone had penetrated its computer system by simply guessing a password, which is known in the professional jargon as a "brute force" attack. In this case, the attacker stopped at the Twitter post and thus the damage was relatively limited. The most astonishing thing about the incident was that four Syrian hackers who belonged to the Syrian Electronic Army were discovered to be behind the breach. Their attack was an expression of the tension that existed between the US administration led by President Obama, and Syria, regarding the latter's use of chemical weapons.

The main insight from this incident is that four people (in this case, Syrian) lacking the capabilities of a superpower, demonstrated the potential to cause economic damage to the leading global superpower. This was not a penetration of the stock market's computers or of the American banking system; rather it was an attack that had a psychological impact. Thus, when characterizing the type of critical infrastructure that should be protected and the means of protection, public confidence should also be seen as a type of critical infrastructure needing protection. In this regard, it should always be assessed what the adversary, whoever it is, could do, via cyberattacks and by penetrating computer systems and computer networks, in order to undermine public confidence.

The asymmetry between these kinds of adversaries and states is sometimes to the detriment of the state, which is much more digital, far more dependent on advanced systems, and possesses critical computer-based infrastructure. Stateless terrorist organizations that have cyber capabilities—such as ISIS and Hamas—have an asymmetric advantage as they do not have critical infrastructure, a financial system, or even a public whose confidence must be maintained so that they can govern. Public confidence can be undermined by harming the financial, political, or democratic system. Nothing needs to actually collapse in these systems; rather, the feeling that something bad is going to happen to them is enough. This problem is even more complex in the cyber age, as the attack surface is expanding. These scenarios keep the National Cyber Directorate up at night.

Additional threat profiles that should be taken into account relate to the spread of superpower attack tools. The best example of this occurred in May 2017 when North Korea obtained a cyber tool attributed to the United States (Eternal Blue), which was leaked out of the labs of the National Security Agency and then used in a worldwide ransomware attack. The United States

was itself attacked, as was the United Kingdom. An official British report on the attack indicated that 139 urgent surgeries in the British health system had to be postponed as a result and damage was estimated at £2.5 billion. Unlike nuclear weapons, which so far have fallen into the hands of terrorists only in Hollywood movies, the leakage of superpower cyberattack tools has already occurred in reality.

As for cyberspace, all the players have capabilities, if only due to the nature of the cyberspace tools: they are made up of computer codes, which, once launched, are not usually destroyed and thus can easily be reused as a "cybernetic warhead," much more than a kinetic warhead that did not explode—provided that the weapon was not obtained first by leaking it from its production lab, as in the American case. Hence, Israel is exposed to the use of superpower tools against it.

Other threat profiles, beyond the scope of this paper, are threats to the supply chain and its defense, as well as cybercrime. It should be noted that the distinction between cybercrime and cyber threats to national security is becoming blurred as more criminal groups work for foreign governmental and military bodies. All these trends and threat profiles demand awareness and all possible means of action in order to protect against them.

Israel was one of the first countries to identify these trends and threats. As early as 2002, protection of computer and information infrastructure was defined as critical and vital, and the task was assigned to the Shin Bet. A decade later, the State understood that more was necessary, and in 2012, on the initiative of Prime Minister Netanyahu, a national directorate was created to address strategy and all aspects of national cyber issues. Two years later, the need arose for a separate operative authority that would handle cyber events in the civilian sphere, and in 2016 the National Cyber Security Authority was established. The State very quickly understood that these two support units should not operate separately or even competitively, and in January 2018, they were merged into a single directorate—the National Cyber Directorate—whose first and foremost task is protecting Israeli cyberspace.

The National Cyber Directorate's second task, which is closely connected to the first, is furthering Israeli leadership in the global cyber arena. The State of Israel has created a unique cyber ecosystem that incorporates the government, academia, and industry, based on the conception that investment in human capital and industry are necessary for maintaining high-quality

protection and superiority over time. Israel and its National Cyber Directorate have established six academic research centers in partnership with various universities and have developed a model for advancing and investing in the Israeli cyber industry, which contributes to the state, to society, and to the economy, and thus to national resilience in general and cyber security in particular.

The position of Israel's cyber industry is manifested in the annual survey of 500 leading companies in the field known as the Cyber Security Ventures. It covers 354 American companies, followed by 42 Israeli companies. The United Kingdom is ranked third, with half as many companies as Israel, followed by a long list of companies from various other countries. According to the survey, there are another 40 or so Israeli companies that are located in Israel but registered in the United States for tax and trade considerations. Thus, the real numbers are about 310 American companies versus 80 Israeli companies; i.e., four times as many, whereas the ratio between the economies and populations of the two countries is much higher.

Israel has succeeded in developing a cyber security strategy that includes three layers: durability, resilience, and national defense. The durability layer is akin to hygiene, a kind of hand washing before eating in order to stay healthy. Investing in this layer is cheaper than investing in the next layers. Regulation is aimed mainly at this layer. The resilience layer is based on the assumption that attacks will occur, and in order to recover from them as quickly as possible and with as little damage as possible, we should prepare accordingly. The third layer, in which the National Cyber Directorate is not at all involved, handles and thwarts attackers. The Israel Defense Forces and the other defense institutions are the ones who deal with this, although the National Cyber Directorate is a partner in the effort by assisting, guiding, and providing information.

This is the strategy underlying the National Cyber Directorate. It operates a national emergency center for handling cyber events, which operates twenty-four hours a day, every day of the year. This is the national CERT (Computer Emergency Response Team) facility, which is located at Cyberspark in Beersheba. Any citizen and organization that suspects that it has been cyber attacked can contact the center and receive assistance and guidance.

Israel has many independent cyber capabilities on the level of a superpower. Nonetheless, international cooperation is still a vital need for Israel. Thus,

the Cyber Directorate works in cooperation with over seventy emergency centers around the world to handle cyber events. It is also a member of and takes part in international cyber forums and is a partner in the assistance programs of various organizations such as the World Bank, the Development Bank of Latin America, and others. Cyber cooperation aims first of all to address operative and defensive needs. Those who attack Israel, such as Iran, do not do so directly but instead via other countries, most of them friendly toward Israel. The more connections Israel has and the more it creates a shared language with these countries, the easier, better, and more effective the work of defense and deterrence will become.

Cyber security in civil aviation, in which the National Cyber Directorate leads and has invested considerable effort, is a good example of international cooperation between forces. It aims to address phenomena connected to the modernization of aviation, which in itself is a welcome development. Passenger aircraft such as the Dreamliner and the Airbus 380 are high tech. Today, flight plans for the newest aircraft, as well as for older ones, are received via tablet computers and not in writing as in the past. This is only one example of possible cyberattack avenues. In order to be prepared for such attacks, the Directorate facilitated the establishment of a consortium of Israeli companies, led by Israel Aerospace Industries and including companies such as Check Point and El Al, to develop and provide solutions in this area.

The National Cyber Directorate's focus on cyber security in civil aviation combines its two main tasks: protecting Israeli cyberspace—in this case, civil aviation and airports in general, which are defined as critical infrastructure—and furthering Israel's global cyber leadership. The combination of aviation, security, and cyber considerations directly connects with Israel's strength and its comparative advantage.

Without ignoring the current public discourse on protecting the democratic process, the National Cyber Directorate focuses on a cyber-technological orientation and carries out a comprehensive systemic assessment well before Election Day. The directorate works in cooperation with the Central Elections Committee on the vote-counting process, which is just a tiny piece of the entire process. In addition, the directorate provides the entire economy, the media, the polling institutes, and additional organizations through which public opinion can be influenced, with recommendations for protection

in cyberspace in order to ensure that Israel's democratic process is free of foreign influences and unwanted interference in various cyber scenarios.

In democracy, there is a separation of powers; in cyber, it is customary to talk about a separation of networks. The National Cyber Directorate provides guidance on critical infrastructure that is under the government's responsibility but does not offer guidance to the other government branches, such as the legislative or judicial branches. It would not be appropriate to do so in a democracy, and the Cyber Directorate takes this very seriously. In this way, the government (via the Cyber Directorate) refrains from instructing the Central Elections Committee, the Knesset, or the State Comptroller on cyber issues, and instead works according to the model of "voluntary guidance;" i.e., voluntary cooperation in sharing knowledge, which works well. These bodies decide independently what they do in cyberspace and in terms of their cyber security. The National Cyber Directorate provides them with the knowledge, intelligence, and comprehensive support needed in order to succeed, each in its field and in accordance with its area of responsibility.

The National Cyber Directorate is currently working on developing a national defense architecture through a multi-year, advanced technological perspective, at the end of which it will be possible to share as much information as possible with partners in Israeli cyberspace and succeed in the early discovery, identification, and elimination of cyberattacks. The cyber law that the National Cyber Directorate is promoting is a critical tool for the success of Israel's cyber security. To this end, the Cyber Directorate also supports the international cyber coalition with senior officials in many countries that are friendly toward Israel.

The guiding principle of the National Cyber Directorate is collaboration, creation of partnerships, and expanding the circle of defense partners, as no single body—no agency, government ministry, or state—can cope alone with the enormous challenges which have been briefly reviewed here. United we stand strong; divided—we fall.