Strategic Trends in the Cyber Realm

David Siman-Tov

With the world already moving to a digital environment, digitalization processes accelerated during the COVID-19 crisis, along with increased dependence of the economy and individuals on centralized computer services. As such, the physical world has become more vulnerable and sensitive than in the past to glitches or malicious attacks. Indeed, a rise in the extent and variety of hostile cyber activity is evident. Accordingly, the challenge of protecting both national and civilian cyberspace has grown.

The past year saw an increase in the range and scope of cyberattacks, launched for strategic purposes such as espionage and disruption of systems; economic and cognitive purposes; and even attacks on information security companies. The level of cybernetic tension between countries has expanded, and the activity and audacity of online criminal elements has also increased. In turn, there has been a more active and aggressive response on the part of cyber authorities in the attacked countries. Against this backdrop, cyberspace has become a realm of strategic conflict. The rivalry between the United States and other countries, especially China, Iran, and Russia, has intensified and in part become overt. Cyberspace as a conflict arena also includes Israel, and in the summer of 2020 Israel and Iran exchanged cybernetic strikes. In fact, cyber is going to become a central component of Israel's strategic campaign between wars.

Against the backdrop of the COVID-19 pandemic, there has been a dramatic increase in cyber and disinformation attacks on health systems and vaccine development efforts. In addition, given the intensive transition of many economic sectors to remote work and remote consumption, the digitalization process has accelerated, but in a way that is unplanned and disordered. Consequently there has been a considerable increase in the use of digital infrastructure, especially cloud services, which constitute a central target for attack. Hence there is a need for an appropriate cyber architecture for the era of working from home and online consumption, which is expected to remain in place even after the pandemic is contained.

In the economic arena, there was a 300 percent increase in cyberattacks in 2020 over the previous year, especially ransomware attacks, which are carried out by state or criminal actors. The general response of the attacked country is a refusal to accept the demands of the attackers, along with greater active operations against them. However, it is difficult to enforce a binding policy in this respect, and many surrender to demands. One of the results of the increased scope of attacks of this kind is a considerable spike in cyber insurance prices.

A central target for cyberattacks, combined with disinformation campaigns, is election processes in Western countries. As a lesson from Russia's attempt to influence the US presidential elections in 2016, national cyber organizations and social media companies helped thwart influence attempts, which thus occurred to a lesser extent in advance of the 2020 presidential elections than in previous elections. This trend of disrupting democratic processes is expected to continue and become even stronger, in both election campaigns and in the periods between them, through extensive activity on social media, the use of technological attack capabilities, and the contamination of the discourse.

The developing capabilities of artificial intelligence and of the Internet of Things – which are apparent, for example, in vehicles, drones, smart cities, and smart homes – create the potential to attack, disrupt routines, and threaten lives, and this demands appropriate defensive preparation. Artificial intelligence capabilities can also be harnessed for defense, but they have not yet been translated into concrete uses.