**The April cyberattack on Israel's water facilities - An analysis / Omree Wechsler**

According to an internal report, a chain of cyberattacks targeted several water facilities and waste management systems. On April 26, Ynet News, Israel’s largest media publication, reported that the attack was thwarted, however possible damage could result in lasting implications.

**What is it all about?**

Operational Technologies (OT) are used to monitor, manage and control physical devices as well as processes in industrial environments and critical infrastructure, which includes power stations, nuclear reactors, sewage treatment facilities and satellites. Along with technological advancements, more of these systems were brought online in order to enable remote access capabilities and operations. However, the increasing connectivity also renders them vulnerable to cyberattacks. Cyberattacks on OT systems requires accurate intelligence and preparation work and is not an easy task for an attacker. However, these attacks may cause a significant, physical damage. Another possibility is that the reported incident is a part of reconnaissance activity aimed in order to gain information on the structure of the system. This can enable a second attack which involves the use of specialized malwares.

Cyberattacks on the OT systems themselves are rare. The first reported attack on these systems took place in 2010 when the Stuxnet worm which according to foreign media reports was developed by Israel and the U.S ultimately sabotaged Iran's uranium enrichment facility at Natanz. In 2014, a cyberattack caused a meltdown in a German steel mill. In 2015 and 2016, Russian hackers disrupted electricity supply to more than 250,000 citizens in Ukraine. Israel has also witnessed failed attempts to attack its OT systems. In 2013, Syrian hackers attempted to attack Haifa’s water infrastructure.

**Who is behind the recent attack?**

While cyber criminals have successfully attacked critical infrastructure in the past, cyberattacks on OT systems require considerable preparations and technological prowess. Therefore, all the known OT cyberattacks were attributed to nation states and foreign military and intelligence organizations. Former NSA and CIA director Michael Hayden compared Stuxnet to the dropping of the atomic bomb in Japan. Hayden warned that exposing capabilities to execute cyberattacks in order to cause physical damage will result in other countries adopting similar capabilities and tactics. Since 2010, most cyberattacks on OT systems were attributed to Russia as it continues to develop offensive cyber capabilities in order to deter and weaken strategic rivals or countries of strategic significance to its national interests, such as Ukraine.

Iran has also become a leading regional power in the cyber sphere. Since 2010, Iran has admitted several times that the Stuxnet attack had shifted its focus towards offensive cyber capabilities. Since then, Iran has invested many resources into further developing defensive and offensive cyber capabilities. In the last couple of years, Iranian hackers have targeted dozens of energy companies, petrochemical facilities, as well as oil and gas pipes in Saudi Arabia, Kuwait and the UAE. As destructive as they were to computer systems, these attacks have all targeted the administrative networks of the facilities. However, this trend started to change in late 2019. According to a warning which was published in December 2019 by Microsoft's security researchers, Iranian hacking group APT33 was spotted targeting industrial control systems that are typically used in the energy sector.

**How should governments address the threat to OT systems?**

In recent years, governments have published warnings as well as guidelines on how to manage cyber risks on critical infrastructure. Many governments, academic institutions and private sector representatives have been attempting to declare cyberattacks on critical infrastructure as a violation of international law through norms-building processes at the UN. States, such as the U.K and France, have threatened to respond to these types of attacks with force. The Trump administration has loosened restrictions on the use of offensive cyber capabilities and has developed the concept of "Defend Forward" which entails the proactive pursuing and countering of adversaries in foreign networks. In June 2019, the New York Times reported that the U.S Cyber Command has infiltrated Russia's national power grid as a response to previous Russian attempts to infiltrate critical infrastructure in the U.S. This leads to the following question: What are Israel's options?

The rapid response of the Israeli National Cyber Directorate, which is responsible for the cyber security of critical infrastructure in Israel has apparently prevented significant damage. It is likely that the attackers took advantage of the fact that Israel is immersed in the fight against the Coronavirus and attempted to cause physical damage such as disrupting water supply, or even worse, adding chlorine to water wells.

Israel's cyber capabilities are much more advanced than the capabilities of it adversaries. Therefore, Israel should use its prowess in order to deter, disrupt and preempt adversarial activities in cyberspace.

Omree Wechsler is a senior researcher for cyber strategies in the Yuval Ne'eman Workshop for Science, Technology and Security in Tel Aviv University.