THE EVOLVING THREAT FROM CYBER TERRORISTS

Terrorist organisations intent on destroying their enemies are using increasingly sophisticated cyber attacks to damage critical infrastructure and kill large numbers of people, according to a former Israeli security chief

Governments and large organisations trying to protect themselves from large-scale cyber attacks face two primary challenges in the modern era, according to Doron Bergerbest-Eilon, the former Head of the Protection and Security Division of the Israel Security Agency and Israel's most senior ranking security official.

The first is the constantly evolving nature of the terrorist threat. In the past, terrorists were primarily motivated politically, by the aim of ousting governments and installing new regimes. They were not looking to inflict mass damage or casualties which might have eliminated the possibility of negotiation. However, the upsurge of terrorist organisations like al Qaeda and ISIS which have set their sights on the complete destruction of their opponents has dispelled this constraint.

'The objective of Mohamed Lahouaiej-Bouhlel, the perpetrator of the lorry attack in Nice on Bastille Day in July 2016, was to cause as many casualties as possible. A total of 86 people were killed in that attack and hundreds of others were injured.

'And in September 2001, we know that al Qaeda sought to inflict as many casualties as possible when they carried out multiple attacks on US targets. The two World Trade Center towers at 110 storeys each could accommodate up to 50,000 workers and an additional 200,000 visitors daily, an extraordinarily large number of potential casualties to target.'

The second challenge is the evolution of cyber warfare itself. When it started in the 1980s, the aim of the Soviets was to steal software and information from the US. To combat the threat, the US planted malware to disrupt its use.

'Today, cyber warfare is increasingly aimed at damaging a country's or company's critical infrastructure, and in some cases to cause mass casualties. For example, cyber attacks can cause massive damage, loss of life and widespread confusion and panic by shutting down cellular services, switching off power plants or water treatment plants, corrupting ATMs, rerouting train lines or switching off traffic lights – just to name a few.

'In fact, many reports today go so far as to indicate the likelihood that future wars may be predicated upon cyber attacks involving communications, energy or financial services.'

During Doron Bergerbest-Eilon's distinguished career with the ISA, he held a number of senior positions, including responsibilities over securing Israel's air, land and sea borders. In addition, he was in charge of the protection of national classified information and national critical infrastructure. He founded the National Cyber Authority for the Protection of Israel's Critical Infrastructure, the first agency of its kind in the world, and was actively involved in developing a national strategy for information security and critical infrastructure against cyber threats.

After retiring from public service in 2005, he founded ASERO Worldwide, which offers a wide range of consultancy services for private and public sector clients on relevant homeland security topics. These include preparing for, mitigating and recovering from terrorist threats, and critical infrastructure protection with an emphasis on cyber threats. ASERO lists among its prestigious clients government agencies in the US, Canada and Singapore as well as private companies such as Mars Incorporated, the AES Corporation and Delta Air Lines.

He says that the key principles for securing any infrastructure or facility can be broken down into three interconnected sectors: physical security, cyber and IT security, and emergency and recovery preparedness. 'Security often fails when we focus our efforts or our resources too strongly on one principle while neglecting the others.

'For example, we estimate that 60 per cent of cyber attacks are caused by 'insiders' such as disgruntled current or former employees. If we secure computer systems only, we neglect to vet employees properly, install and safeguard passwords, or secure server rooms to prevent unauthorised access. In addition, non-cyber threats such as the air conditioning inside a server room can be manipulated to corrupt or disrupt data services.

'It is also necessary to understand the specific needs of a client and the threats they are facing – defining the threat criteria. To do that, we have to look first at who and what we are trying to protect against, such as an attack by a country, specific organisation or individual, and their capabilities and likelihood to carry out different types of threats.'

It is increasingly difficult to prevent or deter cyber threats, says Doron Bergerbest-Eilon. Unlike conventional warfare or terrorism in which the enemy or attacker can be seen, it is often difficult to identify the source of cyber attacks, making it difficult to retaliate.

When the need for cyber security first emerged, security practitioners attempted to mirror best practices from the physical domain by isolating and safeguarding critical data and information infrastructure. But with up to 60 per cent of attacks coming from within, attempts to isolate infrastructure from outside enemies are futile – while infrastructure relies on communication with other systems for efficiency and maintenance.

Security challenges fall into three broad groups: physical security, cyber and IT security, and emergency and recovery

'So security practitioners responded in the same way as people attempting to thwart attacks since the Middle Ages have, by constructing walls – firewalls for the cyber domain. However, we have learned throughout history that an adversary will find a way to circumvent security measures, including bypassing firewalls.

'Antivirus software was then introduced and widely installed. Yet this did not provide the level of security originally envisioned, as an adversary could develop new viruses capable of evading antivirus software.'

It is clear, he says, that attempts to defend against cyber threats have largely failed, as new ways are continually found to circumvent measures or attack infrastructure. Since focusing on defence will always fail against a determined adversary, a new cyber protection paradigm is needed.

For critical infrastructure, that is provided by industrial control systems (ICS) which have evolved to become some of the most sophisticated technologies available. If ICS can protect against all known scenarios, there should be no real threat from nations, hostile groups or individuals to critical infrastructure managed by those systems.

'For example, driving a car without coolant could eventually destroy the engine. But if the car is managed by a control mechanism, a warning that the car is overheating should appear on the dashboard indicating that you should refill the coolant. Even if you ignore the dashboard warning, more modern cars will take measures automatically to prevent you from destroying the engine.

'The same principle may be applied to critical infrastructure. If a threat is detected, the ICS has the capability to alert relevant channels to take appropriate countermeasures. However, this measure is only successful if the ICS accurately understands the threat and not been fooled into believing that there is no actual threat.'

For example, Stuxnet, a malicious computer worm, was used in 2010 to target the industrial computer systems of Iran's nuclear programme. It is likely that this worm had the capability to deceive industrial control systems and malware detection, making it virtually undetectable. While this capability was once in the hands of cyber superpowers only, today it is probably in the hands of hostile countries, entities and other radicals looking to carry out large-scale infrastructure attacks.

Doron Bergerbest-Eilon argues that not only have adversaries proved their ability to consistently breach cyber defences but that they may also be able to circumvent the most advanced technologies, specifically industrial control systems. This could allow them to destroy infrastructure and cause mass casualties, with serious economic consequences.

His new paradigm would therefore always assume that malware is already inside a system and take steps to protect the integrity of information fed into the ICS – in order to prevent deception that could stop the system from providing optimal cyber protection.