LEARN FROM THE LEADER
87 ONLINE DEGREES FOR NATIONAL SECURITY AND PUBLIC SAFETY PROFESSIONALS
American Military University
APPLY TODAY

# Cyberspace: The New Battleground. A Perspective From Israel

BY JOE CHARLAFF, SENIOR CONTRIBUTING EDITOR

Cyber attacks account for hundreds of billions in stolen funds, compromised IP addresses and damage to mission-critical systems.

Today, every industry sector and government agency is a potential target for cyber attack. In Israel, there are around 1,000 cyber attacks every minute, every day, all day. Some are state sponsored, but most are conducted by hacker groups, organized criminals and terrorists. Israel Defense Forces Chief Lt. Gen. Benny Gantz warned that Israel's future battles might begin with a cyber attack on websites that provide daily services to the citizens of Israel.

Since Israel is heavily dependent on technology, it is especially vulnerable to cyber threats. Indeed, hackers mainly target the country's infrastructure - water, electricity, communications and other vital services. While attackers have so far failed to penetrate major critical infrastructure like the nation's power grid, there's no guarantee it can't, or won't, happen.

## New threats

Liran Tancman, CEO of CyActive, an Israeli cybersecurity company, told *Homeland Security Today* that cyber attacks aimed at stealing and damaging data have developed over the years into a tedious game of cat and mouse between attackers – Black Hat hackers and state espionage programs and defenders – and the IT security industry. The current cybersecurity paradigm is a reactive cycle: if and when a threat is exposed, it is analyzed and a counter-solution is designed with response times varying from weeks to years.

The trouble is that, even after a solution is made available, attackers can easily reuse the original code, modify it and create a brand new version of the threat, evading the newly updated security measures. CyActive specializes in future foolproof malware detection and prevention.

Tancman explained that by reusing code and methods when developing malware, thieves and spies gain the upper hand. While new malware becomes cheaper and easier to develop, the tools needed to locate and disable the malware are becoming more expensive. And all the while, defenders need to cover a growing array of potential targets, each with their own set of weaknesses.

"Thus, for every dollar spent by Black Ha: hackers, hundreds of dollars are spent by the IT security industry. This economic imbalance is the springboard from which cyber crime, cyber terrorism and cyber warfare are launched," Tancman said.

## Cyber intelligence

Today, the sophistication of cyber terrorists and criminals has reached such a high level that it is no longer sufficient to rely on conventional methods of protection against cyber attacks. With the ability to find a way around any new device, it is no longer effective to take preventative action after an attack. Instead, more and more companies and government institutions are relying on cyber intelligence to detect threats before they happen.

The cyber intelligence world has undergone dramatic change in recent years. Growth in traffic, online platforms, applications, devices and users has made the intelligence gathering process much more complex - and challenging.

Gadi Aviran, CEO of SenseCy, one of the leading cyber intelligence companies in Israel, explained to *Homeland Security Today* how critical a role cyber intelligence plays in cybersecurity.

He explained that while the cybersecurity market is growing, growth in conventional defensive appliances, such as firewalls, is slowing down and that something else is replacing those devices to overcome their limitations.

"We harvest a lot of information that is relevant to our customers and their products and we quickly package them into actionable intelligence products starting from early warning alerts," Aviran said.

During the last four years, security professionals in organizations have begun to understand the limitation of an appliance. Target, for example, had every security appliance available on the market, including a large IT and security staff, yet a security breach compromised the personal information of millions of consumers.

"Intelligence won't catch all the attacks," said Aviran. "It has its limitations, but provides you with the ability to look ahead."

Aviran views the issue of cyber intelligence as an additional layer of the defense shield. The ability to extract significant deductions from the information gathered allows them to alert a customer well before an attack takes place. In the last three years, there has been a sharp increase in awareness of cyber intelligence.

## Countermeasures

In an attempt to counter the ever-growing cyber threats to critical infrastructure and industry in Israel, a National Cyber Bureau (NCB) was established in early 2012 with the goal of coordinating a strategy to meet the present and future challenges from hackers and states-ponsored attacks. The focus is on building a national cybernetic defense concept and advancing regulation nationally to create a raised level of cybernetic defense. The principal goal of NCB, though, is to build an advanced technological infrastructure incorporating surveillance and to encourage industry to participate in developing a cyber defense system capable of warding off enemy attacks.

Since 2012, several developments have taken place. Daniel Cohen, senior researcher at the Institute for National Security Studies in Tel Aviv, told *Homeland Security Today* that, "Perhaps the most significant has been funding of cyber research programs. I think that in a year or two from now we will see progress from these funds that could help cyber policy and better cybersecurity technology." In addition, work has begun on the establishment of a Computer Emergency Response Team (CERT).

## Cyber defense in the IDF

Israel is one of the first nations in the world to establish a situation room devoted entirely to cyber defense. This situation room, which was established two years ago, is part of the operational preparedness goal of the Israel Defense Forces (IDF) to maintain consistent and regular activity based on IDF's spheres of cyber activity in the air, sea and land. IDF comes under the command of the C4I unit, which protects all IDF IT capabilities and the military's computer systems 24 hours a day, working with local cyber defense teams to assess threats.

Major Oron Mincha, head of International Affairs and Public Affairs for the C4I division of IDF, told *Homeland Security Today* that, "It is equivalent to the J6 in America and is the youngest directorate of the IDF, established in 2003 incorporating the signal corps, the IT and technological division of the IDF. Under this command is the electronic warfare center, cyber defense department, satellite communication and networks.

In the last two years, Israel has seen an increase in attempts to attack its systems and facilities from the north, including daily attack attempts by the Syrian Electronic Army (SEA). The threats are aimed at disrupting Israel's defense and attack capabilities. By the end of 2013, with Iran's assistance, Hezbollah's cyber capabilities improved dramatically.

"One of our main advantages is that we have unique people from the ages of 17 to whom we provide a boot camp-style training for four months studying 12 hours a day to become outstanding defenders of the cyber domain, " Mincha said.

Elite cyber teams, termed blue and red, possess a variety of capabilities to ensure defense walls are defended. They form the special forces of Israel's cyber domain. Their capabilities were developed within their own units to detect and intercept cyber threats. And the threats are not getting easier and attempted attacks are daily, Mincha said. Every Holocaust Day and Independence Day, groups like Anonymous increase their attempts to hack into Israeli government and military computer systems.

"With our technological capabilities and manpower, both men and women, it can be said that so far that we believe the IDF has the edge on its enemies, but we can never for a moment be complacent and let our guard down," Mincha stressed. "We have to be on the alert 24/7. Never underestimate your enemy."