

# Israeli hacking school trains cyber warriors

December 2 2013, by John Davison

---



Trainees work at the "Cyber Gym" centre, where IT and infrastructure company employees train to defend against cyber attacks near the Israeli city of Hedera, on October 30, 2013

Three hooded hackers hunch over their computer screens in the control room at Israel's new state-of-the-art "Cyber Gym", where IT and infrastructure company employees train to defend against cyber attacks.

The facility, a series of small buildings in the shadow of the looming Orot Rabin power station on Israel's northern coastline, was inaugurated

this month by the Israel Electric Corp (IEC), which has experienced its fair share of cyber attacks.

"Israel, we believe, is the most-attacked country," Cyber Gym director Ofir Hason told AFP.

"And as the most-attacked civilian company in Israel, this gives us the unique capabilities to train other companies around the world" to defend against system hacking.

IEC itself is subjected to some 10,000 attacks per hour, CEO Eli Glickman said, and the Cyber Gym's instructors are well-versed in the art of [cyber warfare](#).

"We're a group of professionals from the army, security services and (straight) from university," said an instructor who called himself "Mister" and refused to show his face on camera.

Mister launches simulated attacks against the computer systems of the trainees, who sit in an adjacent building.

"It's a playground to simulate real cyber attacks," he said while seated in the "attack room"—a computer nerd's paradise, decorated with Star Wars and Pac-Man murals and lines of code running off wall-mounted screens that show the hacking taking place live.

But the work is serious—Cyber Gym's launch was attended by members of Israel's intelligence community—and is designed to put trainees under as much pressure as possible.

Trainees—mostly IT and systems workers from energy and infrastructure companies—sit in the "defence room" experiencing the hacks in real time, and their progress is scrutinised by another instructor,

who refers to himself only as "A".

"Each attack is different, so there's no way for the defence teams to cheat. There's no set scenario or scripted attack; they're performed in a different way, live, by the hackers next door," he said.

"If the hackers succeed, the lights go off and the system shuts down," he says, in what is a simulation of just one potential result of a successful attack.

Plunging the room into darkness is one of a number of ways the centre shows the practical outcome of a cyber attack, which can often be forgotten when the fight is conducted in the ether.

"An attack could end with damage to equipment, or a blackout around Israel," Hason said.

"In the cyber arena, when you fail to protect your system, the influence could be physical damage to your system."



Trainees work at the "Cyber Gym" centre, where IT and infrastructure company employees train to defend against cyber attacks near the Israeli city of Hedera on October 30, 2013

### **'Future battle will be in cyber space'**

Israel's politicians and generals often warn of the dangers of hacking.

Last month, the armed forces chief of staff painted a grim picture of a future war in which the Jewish state comes under simultaneous attack both on the ground and in [cyber space](#).

"It is possible that there will be a cyber attack on a site supplying the daily needs of Israeli citizens; that traffic lights would stop working or the banks would be paralysed," Lieutenant General Benny Gantz told a security conference in October.

Around the same time, the Israeli security services reportedly thwarted a [cyber attack](#) and an attempt at industrial espionage that originated in China.

And in June, Prime Minister Benjamin Netanyahu accused arch-enemy Iran of stepping up cyber attacks against Israel, including through its Lebanese ally Hezbollah.

But Cyber Gym and IEC executives were tight-lipped about where most of the attacks against their systems come from.

From "all over the world", said Glickman, declining to give specifics.

Energy Minister Silvan Shalom, who attended Cyber Gym's inauguration, was equally enigmatic.

"We can't give you any specific details," he said.

For now, Cyber Gym is primarily reaching out to Israeli companies, but it is hoping to branch out further.

"There's a possibility it will be opened up to American companies, western Europe, eastern Europe and Asia," IEC vice president Yaakov Haim told AFP.

In the meantime, the trainees are working hard amid a tranquil setting of green lawns and fruit trees laden with unpicked oranges, on the front lines of a new battlefield.

Asked whether Israel was more concerned about a physical or a virtual attack, Shalom said: "I think the future battle will be in cyber space."

Citation: Israeli hacking school trains cyber warriors (2013, December 2) retrieved 26 June 2024 from <https://phys.org/news/2013-12-israeli-hacking-school-cyber-warriors.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.