Israel seeks to export cyber tech, despite risk

January 29 2014, by Daniel Estrin

In this Sunday, Jan. 26, 2014 file photo, Israel's Prime Minister Benjamin Netanyahu attends the weekly cabinet meeting in Jerusalem. At a cyber-technology conference Monday, Jan. 27, 2014, Israeli Prime Minister Benjamin Netanyahu announced a bold initiative calling on tech giants and Western powers to band together to protect the world from cyber-attacks, vowing to relax export restrictions normally placed on security-related technologies so Israeli cyber-defense companies can sell their expertise around the globe. (AP Photos/Ronen Zvulun, Pool, File)

Israeli Prime Minister Benjamin Netanyahu announced a bold initiative this week calling on tech giants and Western powers to band together to

protect the world from cyber-attacks, vowing to relax export restrictions normally placed on security-related technologies so Israeli cyber-defense companies can sell their expertise around the globe. Making this vision a reality, however, will be complicated.

Industry experts say that tech companies and intelligence agencies would likely be loath to trade secrets and reveal their own vulnerabilities. Israel also risks compromising its own national security by allowing cyber companies, mostly formed by graduates of stealth Israeli security units, to export advanced technologies that enemies could use against Israel.

"We are taking a gamble," Netanyahu acknowledged at a cyber-technology conference Monday. "Entailing some risks, but willing to do so to get much bigger gain."

Israel established a national cyber bureau two years ago to coordinate defense against attacks on the country's infrastructures and networks, such as a virus that recently shut down a major Israeli roadway two days in a row.

The bureau also seeks to boost Israel's economy by building up its cyber-defense industry. In the last few years, the number of Israeli cyber-defense companies has ballooned from a few dozen to more than 200, accounting for 5 to 10 percent of the global cyber-security industry, said Eviatar Matania, head of Israel's national cyber bureau.

Matania estimated the global industry to be worth $60 to $80 billion a year. Check Point Software Technologies, one of the world's leading cyber-security firms, was founded in Israel.

"By developing more and more human capital in the area ... we will be able to be a global cyber incubator," Matania said.

This week, international giants IBM and Lockheed Martin announced new cyber research projects in Israel, and Deutsche Telekom and EMC have also established research centers in the country. Hundreds of cyber security companies and experts, including directors of cyber security in the U.S. Department of Homeland Security, attended this week's expo of Israeli security companies and start-ups in Tel Aviv.

Seeking to learn from that Israeli prowess, Symantec, a leading computer security company, hosted a "hackathon" at the expo, inviting Israeli hackers—including some teenagers who ditched high school for the day—to try to pierce through its systems. Ewa Lis of Symantec said the company has hosted similar hacking challenges throughout Europe.

Israel has established itself as a world leader in cyber technology innovation, fueled by graduates of prestigious and secretive military and security intelligence units. These units are widely thought to be behind some of the world's most advanced cyber attacks, including the Stuxnet virus, which attacked Iran's nuclear energy equipment.

Each year, these units churn out a talent pool of young Israelis who translate their experience executing or protecting against advanced cyber attacks to the corporate world. But regulation of the industry to bar Israeli secrets and knowhow from leaving the country—like limits that Israel puts on weapons exports—has been almost nonexistent.

The same is true in other countries: Only last month did Western signatories to the Wassenaar Arrangement, an international treaty that regulates arms sales, move to place restrictions on the cyber technology trade. Israel is not a signatory to the Wassenaar Arrangement, but the country says its weapons trade policies follow the spirit of the agreement.

Israel's national cyber bureau said it is currently formulating rules on

what cyber technologies cannot be exported. Rami Efrati of the bureau said those regulations would be completed within six months.

"I don't think cyber is a secret," said Efrati, who is heading the bureau's effort to boost the Israeli cyber defense industry. "On the other hand we have to be very sensitive about this question, in order to make sure we will have an advantage in such technology."

In 2011, Bloomberg News reported that Internet traffic monitoring software made by Israeli company Allot Communications Ltd. and shipped to Denmark ended up in Iran, Israel's arch-foe. The company denied the charge, and Israel's Defense Ministry later cleared it of any wrongdoing.

Alon Hazay, a former cyber-defense expert in Israel's internal security service, the Shin Bet, who now serves as a private consultant, said he was aware of at least two Israeli startups formed by graduates of Israeli security units whose software contains sophisticated defenses that provide telltale clues of the kinds of sophisticated attacks Israel uses against its foes. He said the companies are working for international clients, with one developing mobile phone security solutions and the other providing security for computers.

Hazay declined to identify the companies. The clues in their products, he said, could potentially help hackers and even state enemies to learn Israeli cyber secrets. The "biggest threat for Israeli intelligence," he said, is the potential that "you're actually helping your enemies help protect their systems," he said.

But in the field of cyberspace, Hazay said, it is difficult to ascertain what technology constitutes an Israeli national security asset. He said it was inevitable that such technologies would make their way to the marketplace.

"The guys coming out of the army are going to make money. The only thing they know how to do is security," said Hazay. "You can't prevent them from using their minds."

Citation: Israel seeks to export cyber tech, despite risk (2014, January 29) retrieved 22 May 2024 from https://phys.org/news/2014-01-israel-export-cyber-tech.html