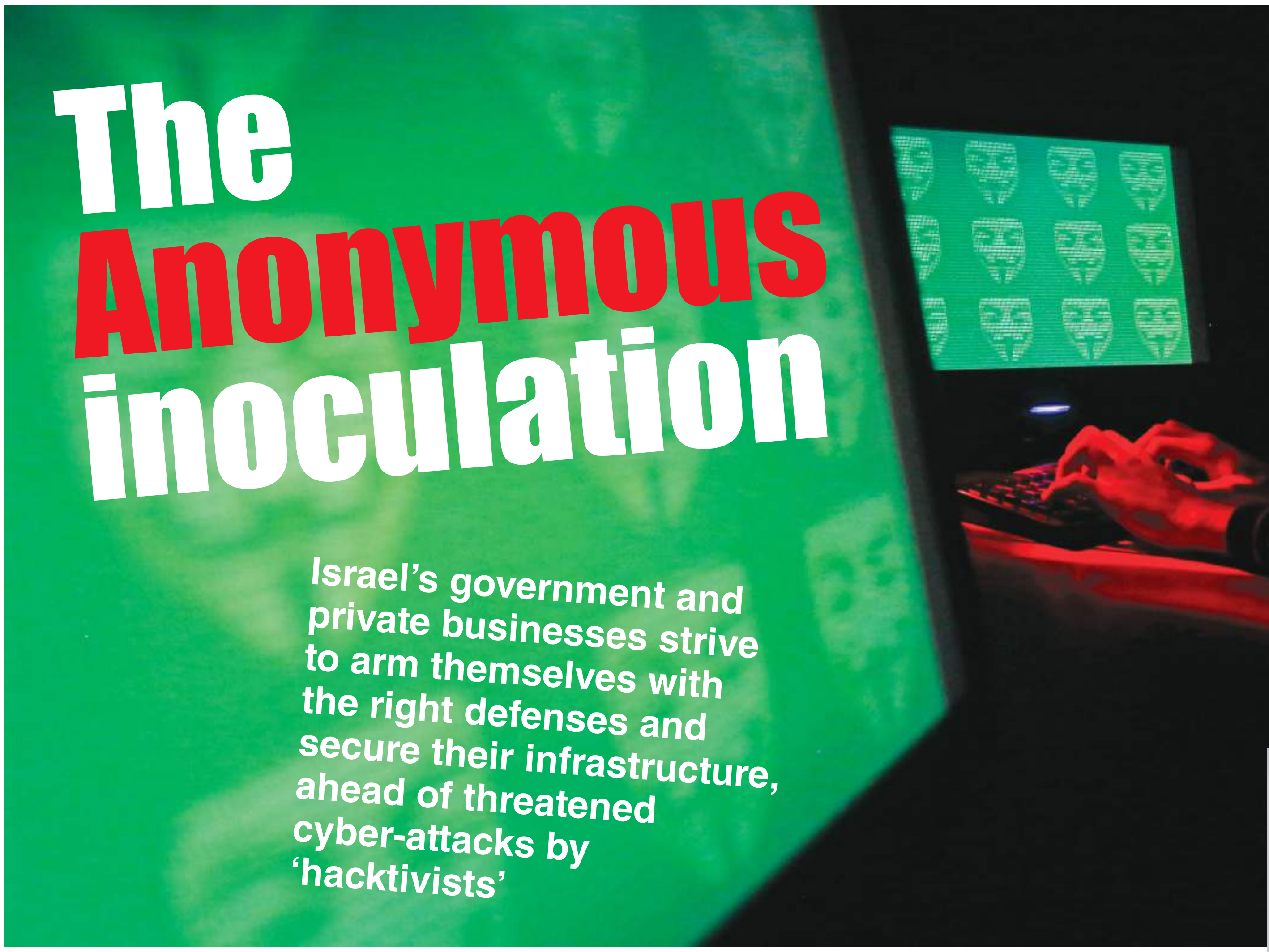
The Anonymous inoculation

Israel's government and private businesses strive to arm themselves with the right defenses and secure their infrastructure, ahead of threatened cyber-attacks by 'hacktivists'



THE LOGO for the cyber hacking group 'Anonymous' is seen on computer screens. (Reuters)

• NIV ELIS

In its third year of coordinating cyber attacks against Israel, the online "hacktivist" group Anonymous decided to up its rhetoric.

On April 7, the group promised in a video, it would unleash "an electronic Holocaust" on the Jewish state, threatening to wipe Israel from the cyber-security map.

"We'll take down your servers, government websites, Israeli military websites, banks and public institutions. We'll erase you from cyberspace as we have every year," said a figure in the video, wearing the stylized Guy Fawkes mask popularized in the film *V for Vendetta*.

The clip, which opened with Anonymous's logo of a headless suit standing in front of a UN-style globe, featured Arabic subtitles, accused "foolish Zionist entities" of "heinous crimes against humanity" and specifically mentioned the death tolls in the 2014 summer war with Hamas in the Gaza Strip, Operation Protective Edge.

Since 2013, the elusive group of politically motivated, loosely affiliated hackers has made similar threats and achieved a modicum of success in disrupting some websites, even leaking Israeli credit-card numbers during its annual "OpIsrael" operation.

This year, it appeared to successfully take down the Education Ministry website, and hacked sites belonging to Zionist Union MK Yossi Yonah, singer Shalom Hanoch and a girls' high school. Other sites the group claimed (via Twitter) to have disrupted, such as an Economy Ministry website, appeared to remain functional.

Sticking with its Holocaust promises, the group attempted to bring down Yad Vashem's website. It was unsuccessful.

Most of the websites were quickly recovered.

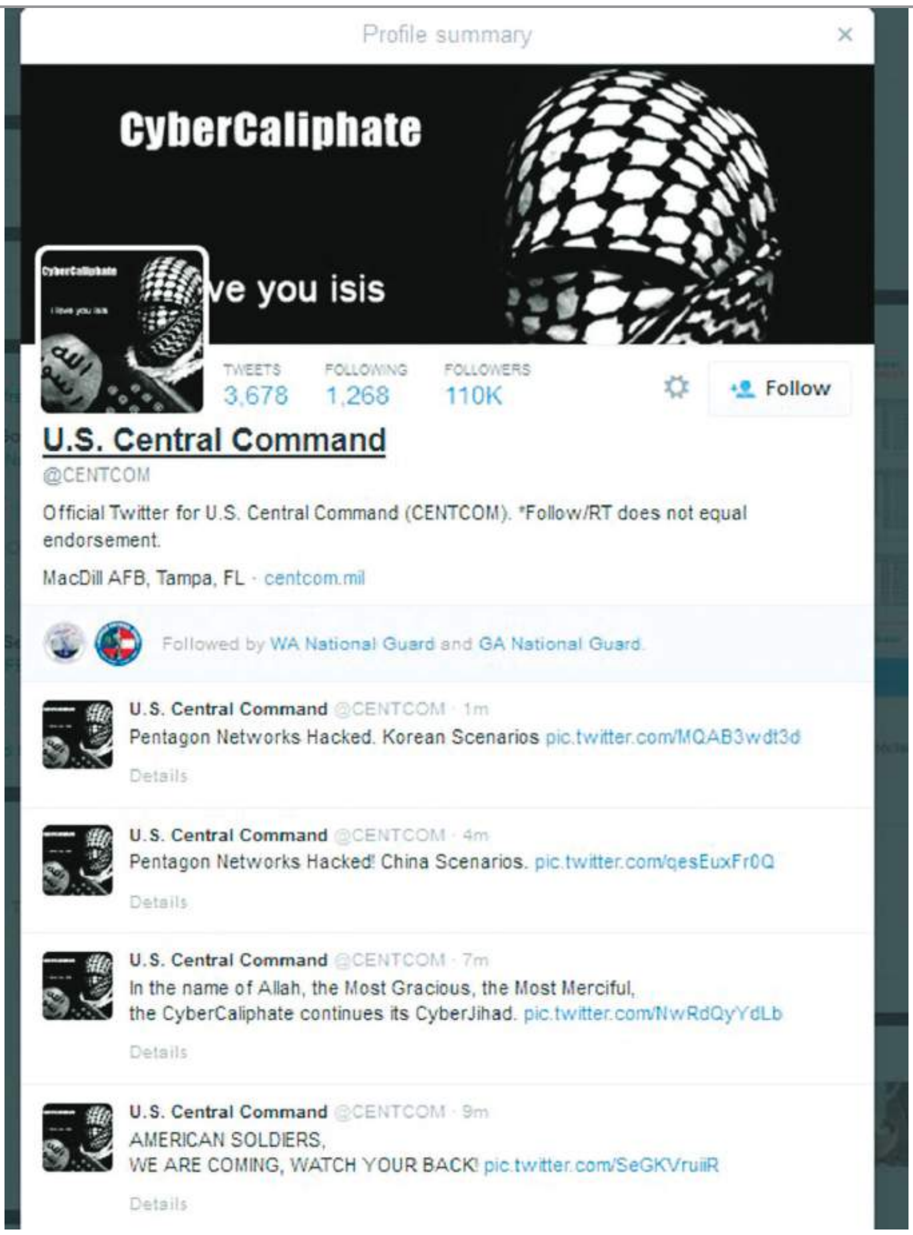
Though Anonymous garnered plenty of media attention, the question is whether it did any lasting damage. Most analysts saw it as a childish nuisance; one pro-Israeli hacktivist even broke into an OpIsrael website and posted messages defending the Jewish state.

"As long as it's a dispersed effort [comprised of] ad-hoc teams getting together for activist causes, I don't see that as a major threat. We should be more concerned about Russia or China, which have real cyber armies," said Asaph Schulman, vice president of marketing at Checkmarx. "It's not like the Chinese trying to hack Lockheed Martin for the latest IP in aerodynamics."

Anonymous has pulled off a few victories through relatively simple hacks and denial of service attacks, which commandeer armies of computers to bring down a website by overwhelming it. But the potential for cyber attacks with real ammunition is far greater.

ASAPH SCHULMAN, the VP Marketing at Checkmarx. (Courtesy)

A MAP of China is seen over binary numbers. Schulman says that cyber-armies from China and Russia are the real threat to national security. (Courtesy)



U.S. Central Command
@CENTCOM

Official Twitter for U.S. Central Command (CENTCOM). *Follow/RT does not equal endorsement.

MacDill AFB, Tampa, FL · centcom.mil

Followed by WA National Guard and GA National Guard.

U.S. Central Command @CENTCOM · 1m
Pentagon Networks Hacked. Korean Scenarios pic.twitter.com/MQAB3wdt3d
Details

U.S. Central Command @CENTCOM · 4m
Pentagon Networks Hacked! China Scenarios. pic.twitter.com/qesEuxFr0Q
Details

U.S. Central Command @CENTCOM · 7m
In the name of Allah, the Most Gracious, the Most Merciful,
the CyberCaliphate continues its CyberJihad. pic.twitter.com/NwRdQyYdLb
Details

U.S. Central Command @CENTCOM · 9m
AMERICAN SOLDIERS,
WE ARE COMING, WATCH YOUR BACK! pic.twitter.com/SeGKVruiiR
Details

A SCREENSHOT of the US Central Command Twitter feed after it was apparently hacked by people claiming to be Islamic State sympathizers. (Reuters)

A MAN holds a flag of the Anonymous hacker group during a protest in Berlin, August 2014. (Reuters)

> *'We're still seeing a lot of resistance and struggle to define what needs to be done at the government level'*
>
> *- Alex Vaystikh, CTO at cyber firm SecBi*

Sure, it's irritating to have your bank's website out of order for a few hours, but in an age where infrastructure is run on computers, there are greater risks.

"That's the next frontier. The damage you can inflict by shutting down the water and electricity, or confusing the traffic control system, is immense," Schulman noted.

"I think Israel is vulnerable. It's all a question of how lucrative a prize there is – if there's enough brain power invested in the idea of attacking Israel, they will find a way to hack into whatever they want to hack."

In April, Col. (res.) Dr. Gabi Siboni, director of the Cyber Security Program at the Institute for National Security Studies in Tel Aviv, told the *Magazine* that "I strongly believe, however, that the next 9/11 will happen without suicide bombers aboard the plane with box-cutters, but will occur because of a cyber incident perpetrated by a terror organization." Nuclear facilities are an obvious target.

Part of the challenge for the government in securing all its data is that there are so many different ways to attack it.

Checkmarx, for example, offers a tool that helps debug programs for vulnerabilities. Everyday programmers are trained to make functional code, not to ensure it's secure. Some hackers can break into the system by simply entering cleverly written code instead of a user name and password.

"Hackers are taking advantages of vulnerabilities in the software, caused by developers who are simply unfamiliar with such tactics," he said. "It's not on their radar."

But that's just one element. CyberArk, another Israeli cyber-security company, focuses on internal threats. WikiLeaks and Edward Snowden's US National Security Agency leaks were both examples of sensitive, damaging information getting out because people with easy access to the information could steal it.

Another major problem is that employees can be tricked into opening a seemingly innocuous email attachment that could plant malware in their company's system. Often, the damaging files will be sent out significantly ahead of a big event, as hackers do reconnaissance and set up elements of a future attack.

In February, a report by Trend Micro stated that Gaza-based hackers launched cyber-attacks against Israeli targets using a pornographic video clip. The operation, which the company called Arid Viper, specifically targeted "a government office, transport service/infrastructure providers, a military organization and an academic institution in Israel," as well as several Israeli individuals and a Kuwaiti academic institution.

CyberReason, a growing cyber firm based in Tel Aviv, aims to map out the entire process of an attack with a visual system, helping identify how threats get in and what damage they do early on.

Part of the problem both the government and private companies must grapple with is figuring out exactly how many companies they need to hire, and what kind of defenses they need to put up to ensure they're secure.

"It's sort of like asking how many insurance policies you need. It all depends on how much you stand to lose if something goes wrong," explained Schulman.

But even if it manages to secure the important infrastructure from smaller-time hackers like Anonymous, the government has limited sway over what happens in the private sector.

"We're still seeing a lot of resistance and struggle to define what needs to be done at the government level," said Alex Vaystikh, chief technology officer at cyber firm SecBi.

The government, of course, cannot protect all the data in the country, and privacy advocates would bristle at the very suggestion. That means that small or young businesses, in particular, which may not have the means or foresight to take proper security measures, are vulnerable.

Ahead of the Anonymous attacks, Israel's National Cyber Bureau and the Shin Bet (Israel Security Agency) set up a system of information-sharing to make businesses aware of threats. IBM has set up a similar intelligence-sharing portal to help spread the word about cyber threats.

"It breaks the asymmetry we've had up until now," said Roee Hay, who leads the team for application security research in IBM's software lab.

But some say that OpIsrael may, perversely, be good for Israel.

Unlike coordinated attacks from enemy states that are meant to cause damage without warning, Anonymous's tactics are more oriented toward raising awareness of their perspective.

According to Vaystikh, part of the reason Anonymous is so unsuccessful in inflicting real damage is that its warnings scare people into preparing themselves.

"I think the side effect of Anonymous is almost boosting security for these organizations," he contended. "It's almost boosting the immune system for the cyber-security ecosystem."

Israel's efforts at inoculating the private sector by making information and resources available on how to secure their data may not be as focused or successful if it weren't for Anonymous's media strategy, which aims to get maximum attention for its cause.

"It is a very interesting paradox going on here that despite their attempts to inflict damage, they're actually boosting security," said Vaystikh. "At some cost, of course, but I think it's actually negligible compared to the benefits of preparing for that attack, for that date." ■