Yuval Ne'eman Workshop
for Science, Technology and Security
Tel Aviv University

ICRC
Blavatnik Interdisciplinary
Cyber Research Center

TEL AVIV UNIVERSITY אוניברסיטת תל אביב

Cyber Israel
National Cyber Directorate

In cooperation with:

Ministry of Foreign Affairs
Israel

ISRAEL CYBER ALLIANCE

State of Israel
Ministry of Economy and Industry
Foreign Trade Administration

ISRAEL EXPORT INSTITUTE

Cyber Week

June 27th-30th, 2022

Tel Aviv University, Israel

Press Kit

PUBLIC RELATIONS (INTERNATIONAL): STRAUSS PR

CAV SPONSORS & PARTNERS

Distinguished Benefactor

THE SAGOL NETWORK

Diamond Sponsors

FORESCOUT

Esteemed Platinum Sponsors

CHECK POINT · IAI · Trellix · YL VENTURES

Platinum Sponsors

BAYER · HOLISTICYBER · IBM · Microsoft · SYGNIA · TEAM8

Gold Sponsors

Checkmarx · CYBERARK · CROWDSTRIKE · ermetic · intuit (turbotax, quickbooks, mint, credit karma, mailchimp) · MANDIANT · MITIGA · SIMSPACE · SYNOPSYS

Silver Sponsors

BioCatch · CYE · Elron Ventures · FORTINET · Google · NTT · NVIDIA · OUTSEER · Synamedia · TEAM CYMRU

Bronze Sponsors

Acronis · amdocs · cervello · CYLUS · cyviation · T · DV DoubleVerify · enav group · CYBER CONTROL · SOMPO Digital Lab Tel Aviv · TREND MICRO

Partners

U.S. Chamber of Commerce · Israel Innovation Authority · ISRAEL TECH POLICY INSTITUTE · CYBER EDUCATION CENTER · CYBTOGETHER · Ministry of Energy www.energy.gov.il · BSIDES TLV 2022 · KONFIDAS · CSAIL cloud security ISRAEL alliance · HiTech Ambassadors · CYTACTIC · UK Israel Tech HUB · TEL AVIV UNIVERSITY · Embassy of the Federal Republic of Germany Tel Aviv · iATI Israel Advanced Technology Industries · CAAI · קרן רשי · משרד הביטחון MINISTRY OF DEFENSE · GLILOT · JETRO · DSI · conexx · BUSINESS FRANCE · RÉPUBLIQUE FRANÇAISE · OurCrowd · FUTURE OF PRIVACY FORUM · GOODWIN · Velvyslanectví České republiky v Tel Avivu Embassy of the Czech Republic in Tel Aviv

VentureBeat

How Israel plans to tackle cyberattacks with a 'Cyber-Dome'

Kolawole Samuel Adebayo

At CyberWeek in Tel Aviv, Israel, Gaby Portnoy, the new director general of the country's Cyber Directorate announced the Cyber-Dome project — a new big data, AI, overall approach to proactive cyberdefense. This project is expected to be a collaborative effort between cybersecurity leaders in Israel and across the globe in preparation for what Portnoy believes is unarguably "the most prominent dimension of future warfare."

In his words, "the Cyber-Dome will elevate national cybersecurity by implementing new mechanisms in the national cyber perimeter and reducing the harm from cyberattacks at scale. The Cyber-Dome will also provide tools and services to elevate the protection of the national assets as a whole ... and will synchronize nation-level real-time detection, analysis and mitigation of threats."

Threats to Israeli cyberspace increase

Although research has proven that every computer system is subject to cyberattack, attacks on a country's government agencies, high-tech companies and defense infrastructure, as well as economic crimes in the million-dollar range are considered "significant" due to their wide-reaching implications. In the Center for Strategic and International Studies (CSIS) latest research, an inquiry into significant cyberattacks per country revealed Israel in the 14th position with 11 recorded wide-scale cyberattacks. What this means is that of the billion-dollar cyberattacks recorded per year, Israel has a large chunk.

For ransomware alone, a review of 80 million samples from 140 countries revealed a 600% increase in ransomware activity, earning the country the least-coveted badge of most-affected by ransomware since 2020. Health institutions were not left out of the digital ambush either, as the Israeli Ministry of Health National Cyber Directorate (INCD) recorded in 2021 a dramatic increase in the degree and quality of cyberattacks on the country's medical sector — with approximately 1,400 attacks weekly.

Fast forward to the first half of 2022 and cyberattackers have already circulated threatening messages through several Israeli news outlets, launched a DDoS attack that led to the shutdown of many government websites, successfully surveilled sensitive members of the country's security establishment, set off air raid sirens in two major Israeli cities and even targeted former government officials like the former U.S. Ambassador to Israel.

Re-creating the Iron Dome effect

Even after stopping 1,500 attacks in the past year, the INCD still believed it was crucial to tighten its cyberdefenses. Just like its skies are protected by its Iron Dome — a multimission, state-of-the-art mobile missile air defense system — Israel has decided to protect its cyberspace with equal sophistication. The Cyber-Dome, an Iron Dome analogy, will be "an ongoing cyberdefense effort to keep the national cyberspace cleaner," according to Portnoy.

In what was his first public speech as DG of the INCD, Portnoy said the first order would be to reframe the challenge by considering the security gaps as opportunities and not problems. By doing this, technology leaders are able to create cybersecure-by-design solutions that would improve the zero-trust approach, he said.

Moving forward, Portnoy emphasized that the project would shift the focus from mere resilience to broadening the defense. This way, agents from the good sides of the three-sided spectrum (attackers, cybersecurity infrastructure and the global internet) are given a level playing field to amp their defenses.

He stressed the "need to protect national assets in the best way possible and make the cybersecurity protocols used for critical infrastructure available for more sectoral organizations in the government and private domains." By providing organizations with better cybersecurity resources like smart identification policies and improving national risk management practices, the attackers would have a harder time completing their missions.

'You cannot fight cyber aggression alone'

In tackling these challenges, the INCD said it discovered there was no single "official enemy." Instead, the attackers ranged from regular attackers to attack groups, proxies, independent crime-organizations and even private people. To build up a defense against these actors, Portnoy stressed that cooperation and mutual responsibility is vital. "You cannot fight cyber aggression alone. You have to have partners, at home, in your defense community, in the government, in the different sectors, in the academy, in the private sector and around the world."

By leveraging the strength of government sector regulators, the security community, the global cybersecurity industry and even citizens, Portnoy is certain that elevating national cybersecurity defense is possible.

CyberWeek is an international cybersecurity conference held annually in Tel Aviv, Israel. It's organized by the INCD and the Blavatnik Interdisciplinary Cyber Research Center of Tel Aviv University.

VentureBeat

Ransomware is still cybersecurity's biggest challenge

Kolawole Samuel Adebayo

Sixty percent of organizations were hit with ransomware last year, according to the Sophos State of Ransomware 2022 Report [subscription required]. With attacks growing in numbers and complexity, and ransom payments rising, the cybersecurity catch-up game keeps raging. As malicious actors continue to exploit and weaponize vulnerabilities faster than ever, Lindy Cameron, CEO of the UK's National Cyber Security Centre (NCSC) notes that ransomware still remains cybersecurity's biggest challenge.

At CyberWeek 2022, the 12th edition of Israel's largest cybersecurity event, hosted in Tel Aviv, Cameron said while it might seem that more sophistication has gone into bolstering security across organizations and nation states in recent years, all hands must be on deck to root out ransomware.

"Ransomware attacks strike hard and fast and they're evolving rapidly. They're pervasive [and] increasingly offered like games-as-a-service, lowering the bar for entry into cyberspace — and that's what makes them such a threat," Cameron said.

As the Russia-Ukraine war continues to rage, cyberattackers deployed ransomware in several instances to serve as a "decoy or distraction" as they targeted organizations in Ukraine. During her speech, Cameron acknowledged the impact of not just the physical assault, but also the cyberattacks.

"The changing geopolitical landscape [has] transformed the context for work in the cybersecurity space," she said, acknowledging the impact of the Russian-Ukraine war on the changing face of cybersecurity. "While Russia is up to this physical oppression, conducting a cyber campaign — which seems to be no surprise — Russia has consistently used cyber pressure to stress its rivals."

Collective responsibility and collaboration

To help quell the onslaught of ransomware attacks, Cameron called for increased cooperation between institutions, technology companies, government and its agencies. She reiterated that "if we're going to maintain a cyberspace which is a safe and prosperous place for everyone, it's vital that such capabilities are produced and used in a way that is legal, responsible and proportionate."

Continuing to sound the beat for collaboration and partnership, Cameron said work must continue in the area of understanding the scale, nature and evolution of the techniques being used in order to make ransomware an unprofitable and unattractive business.

However, her address wasn't all gloom and doom, as she praised the Israeli technological spirit. According to Cameron, the democracies of the world have to challenge themselves to develop technologies and systems which help them to avoid relying on some products not aligned with their values.

"The startup nation of Israel can play an important role in this innovation over the years to come. The technology developed is truly world-class, the talent in the cybersecurity sector is second to none and the defenses are some of the strongest in the world. But making the most of our digital future is too big an issue for any one nation to handle alone. Whether it's feed irrigation or wholesome climate technology, Israel has always been fighting to innovate for the benefit of people well beyond its borders."

Cameron was optimistic that Israel will continue to produce cybersecurity solutions that are safe, strong and affordable for the whole world.

Cybersecurity goes beyond countries and wars

The enterprise is not left out in the battle against ransomware. While countries often get dragged into the mix, the major targets of ransomware are enterprise operators. Recently, IBM X-Force examined over 150 ransomware engagements from the past three years and discovered there was a major decrease in the duration of ransomware attacks on enterprises, specifically the overall time between initial access and ransom requests.

Another trend in the enterprise space is the rise of the initial access broker economy (with "initial access brokers" being the hackers who specialize in breaching enterprises and then selling that access to cyberattackers) and ransomware-as-a-service (RaaS), both of which reduce or totally eliminate the entry barrier to utilizing ransomware. The RaaS industry has become more developed with increasing agility, ensuring that enterprise leaders can't keep up with the rate at which attacks occur.

Beside the need to adopt a zero-trust architectural approach, Cameron notes there must be strong international government policies in place.

"An important part of our response to this as an international community is a thicker issue of enforcement among rules governing activities. If we're to ensure that the digital world remains a place of opportunity and to avoid conflict and struggle, we must be clearer about the guidelines and norms that transcend national borders."

Cameron concluded her session by reiterating that the NCSC is working with partner agencies and organizations to ensure that a society where cyberattacks can be repelled is possible, adding that "cybersecurity is second nature to all of us."

VentureBeat

Immue discovers new exploitation of Apple's private relay

Kolawole Samuel Adebayo

Immue, an Israel-based cybersecurity company providing holistic anti-bot and anti-fraud defense solutions, claims it's found concerning vulnerabilities in one of Apple's latest privacy features — the iCloud Private Relay. While helping organizations across multiple industries stop cyber fraud and bot attacks targeted at their companies, Immue said it detected many of these attacks coming from internet protocols (IPs) associated with Apple and their two supporting Akamai and Cloudflare servers.

In an exclusive interview with VentureBeat at the ongoing CyberWeek Tel Aviv, cofounders Amit Yossi Siva Levi (CTO) and Shira Itzhaki (CEO) confirmed that threat actors take advantage of the anonymity and web browsing privacy features of Apple's technology to mask their IPs and launch multiple untraceable attacks.

Lessons learned from McDonald's, Databricks, and the AI Framework about using amplified intelligence, AI, and machine learning to drive smarter customer experiences_Landscape

Lessons learned from McDonald's, Databricks, and the AI Framework about using amplified intelligence, AI, and machine learning to drive smarter customer experiences_Landscape

How Apple's private relay works

In June of 2021, Apple hosted its annual Worldwide Developers Conference to showcase its latest technologies. Among the technologies launched, the most significant and controversial was the private relay technology which would form part of the iCloud+ subscription. With this service, users on iOS 15, iPadOS 15 and macOS Monterey can browse securely without worrying about having their browsing activities tracked and sold to the highest bidder.

By enabling this feature on an upgraded Apple device, users' browsing activities on Safari are routed through two separate internet "relays" using a sophisticated multi-hop architecture. This rerouting guarantees that no single party — including Apple — can track the exact origin of the request, making it impossible for websites to create a detailed profile of users. Some experts have even called it "internet privacy on steroids."

The exploitation

How private data is managed and shared has always been a concern for the average internet user. Mckinsey reports that internet users are becoming increasingly intentional about the kind of data they share online and with whom, as no industry reached a 50% trust rating. With multiple data breaches springing up globally, many providers and even the government have made efforts towards curbing the menace — so much so that Gartner predicts the personal data of over 75% of the global population will be protected by new privacy regulations by 2025.

The McKinsey report also revealed that these breaches have made users turn to tools that give them more control over their data and its privacy — like the private relay. However, in solving this problem, Apple has inadvertently created a leeway for cyberattackers to thrive.

In what Levi described as "a new kind of attack," he explained that masking IP addresses with proxies, VPN or the Tor network to avoid IP-based detection (like rate limit or IP score) is the single most important rule in cyberattack. He added that in the last two months, Immue has seen attackers abuse Apple's new feature to mask their IPs and send thousands of bots to attack their customers. These private relay IPs are also whitelisted by Apple, giving adversaries uninhibited access to any website. Immue reports the attackers used 192 different IPs to generate three attacks with a volume of up to 50,000 bot requests each time.

Although Apple said the private relay technology was fitted with anti-fraud and anti-abuse systems like rate-limiting, single-use authentication tokens and consistent IP address per browsing session, it advised that fraud detection systems relying only on IP addresses should be updated to control the situation.

Founded in January of 2021, Immue claims its offering is helping different organizations across multiple industries like travel, finance, ecommerce, cryptocurrency and more — to outwit the most experienced human fraudsters and undetectable bots. The company says it offers powerful anti-bot and anti-fraud defense in one holistic solution that mitigates the impact of cyberattacks on businesses.

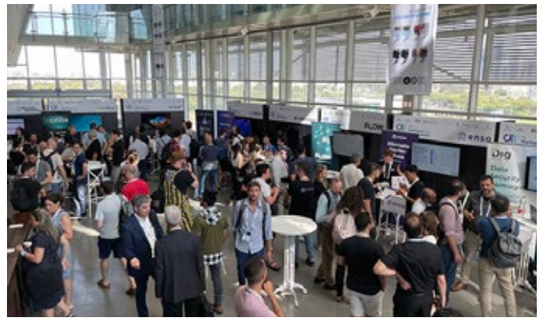
Immue's unique value proposition, according to its cofounders, is its ability to detect cyber threats that no one knows exist. The company does this by monitoring and gathering data about the latest fraud mechanisms, tools strategies and using that information to detect, prevent or stop cyberattacks before they even materialize.

Cyber Week 2022 video walkthrough

Cyber Week is a large annual international cybersecurity event, hosted each year at Tel Aviv University in Israel.

In this Help Net Security video, we take you inside Cyber Week 2022. The featured vendors are: Dig Security, Ermetic, enso, Forescout, Flow, IBM Security, Intuit, Israel Aerospace Industries, Mitiga, and Synopsys.

Photos: Cyber Week 2022



Cyber Week is a large annual international cybersecurity event, hosted each year at Tel Aviv University in Israel. Cyber Week 2022 is held jointly by the Blavatnik Interdisciplinary Cyber Research Center (ICRC), The Yuval Ne'eman Workshop for Science, Technology and Security, Tel Aviv University, the Israeli National Cyber Directorate under the Prime Minister's Office and the Ministry of Foreign Affairs.

The featured vendors are: Acronis, Amdocs, Astrix Security, BioCatch, Bayer, Checkmarx, CyberArk, CrowdStrike, Check Point Software, CYE, Cervello, Canonic Security, Cyberpion, Cylus, CyViation, Dig Security, DoubleVerify, Ermetic, Elron Ventures, ENAV, enso, Fortinet, Forescout, Flow, Google, HolistiCyber, Intuit, IBM, IBM Security, Mandiant, Mitiga, Microsoft, Ness Technologies, NVIDIA, Outseer, RevealSecurity, Red Access, Scribe Security, SimSpace, Synopsys, Synamedia, Sygnia, Sompo Digital Lab, Team Cymru, Trellix, T-Mobile, Team8, Trend Micro, YL Ventures.

Cyber Week
June 27th-30th, 2022
Tel Aviv University, Israel
Yuval Ne'eman Workshop for Science, Technology and Security Tel Aviv University
Blavatnik Interdisciplinary Cyber Research Center
TEL AVIV UNIVERSITY אוניברסיטת תל אביב
Cyber Israel National Cyber Directorate
In cooperation with:
Ministry of Foreign Affairs Israel
ISRAEL CYBER ALLIANCE
State of Israel Ministry of Economy and Industry Foreign Trade Administration
ISRAEL EXPORT INSTITUTE

HELPNET SECURITY

Week in review: ZuoRAT targeting SOHO routers, trends affecting your security strategy

Here's an overview of some of last week's most interesting news, articles, interviews and videos:

OT security: Helping under-resourced critical infrastructure organizations

In this Help Net Security interview, Dawn Cappelli, Director of OT-CERT at the industrial cybersecurity company Dragos, talks about the OT security risks critical infrastructure organizations are facing, offers advice on how they can overcome obstacles that prevent them improving their cybersecurity posture, and explains how the recently set up OT-CERT she's heading can help asset owners and operators of industrial infrastructure.

Cybercriminals use Azure Front Door in phishing attacks

Resecurity, Inc. (USA) has identified a spike in phishing content delivered via Azure Front Door (AFD), a cloud CDN service provided by Microsoft. The identified resources in one of the malicious campaigns impersonated various services appearing to be legitimately created on the "azurefd.net" domain.

Researchers uncover ZuoRAT malware targeting home-office routers

Black Lotus Labs discovered a new remote access trojan (RAT) called ZuoRAT, which targets remote workers via their small office/home office (SOHO) devices, including models from ASUS, Cisco, DrayTek and NETGEAR.

Clearview fine: The unacceptable face of modern surveillance

The UK's Information Commissioner's Office (ICO) has issued its third largest ever fine of £7.5m. It was imposed on Clearview AI, the controversial facial recognition company that has already been on the wrong end of similar decisions from regulators in Italy, France and Australia.

Properly securing APIs is becoming increasingly urgent

Imperva released a new study that uncovers the rising global costs of vulnerable or insecure APIs. The analysis of nearly 117,000 unique cybersecurity incidents estimates that API insecurity results in $41-$75 billion of losses annually.

Detection, isolation, and negotiation: Improving your ransomware preparedness and response

The risks presented by ransomware and cyber extortion events have likely found a place in your own security team's discussions, and rightfully so. Ransomware attacks have proliferated in the last decade.

Trends to watch when creating security strategy for the next two years

Executive performance evaluations will be increasingly linked to ability to manage cyber risk; almost one-third of nations will regulate ransomware response within the next three years; and security platform consolidation will help organizations thrive in hostile environments, according to the top cybersecurity predictions revealed by Gartner.

Why digital trust needs to be a strategic imperative for your company

It's no secret that digital interactions have extended to every aspect of our professional and personal lives. Connectivity is soaring and digital transformation is accelerating, making it critical for the technology community, governments and corporate boardrooms to invest in digital trust.

Destructive firmware attacks pose a significant threat to businesses

As business workforces become increasingly distributed, IT leaders say it's harder than ever to defend against firmware attacks, according to HP Wolf Security.

Evolving online habits have paved the way for fraud. What can we do about it?

Information is power, and personally identifiable information (PII) is an extremely powerful asset that is fueling the rapid growth of online fraud (also known as the Digital Identity Crisis).

Threat actors increasingly use third parties to run their scams

Abnormal Security released new research that showcases a rising trend in financial supply chain compromise as threat actors impersonate vendors more than ever before.

How phishing attacks are becoming more sophisticated

In this video for Help Net Security, Joshua Crumbaugh, CEO, PhishFirewall, talks about how cybercriminals are taking their phishing attacks to a new level.

48% of security practitioners seeing 3x increase in alerts per day

Panther Labs surveyed 400 active security practitioners, primarily, security analysts and security engineers, to reflect the "boots on the ground" perspective for security teams.

Python packages with malicious code expose secret AWS credentials

Sonatype researchers have discovered Python packages that contain malicious code that peek into and expose secret AWS credentials, network interface information, and environment variables.

EMEA continues to be a hotspot for malware threats

Ransomware detections in the first quarter of this year doubled the total volume reported for 2021, according to the latest quarterly Internet Security Report from the WatchGuard Threat Lab.

Exploring the insecurity of readily available Wi-Fi networks

In this video for Help Net Security, Andy Thompson, Global Research Evangelist at CyberArk, talks about Wi-Fi security.

How parents can talk about online safety and personal info protection with their kids

In this video for Help Net Security, Jim Ducharme, Chief Operating Officer at Outseer, provides insight into how parents can talk about online safety and personal info protection with their kids.

Key takeaways from RSA Conference 2022

In this video for Help Net Security, Ravi Srinivasan, CEO of Votiro, talks about his experiences during RSA Conference 2022.

How businesses are prioritizing data privacy

In this video for Help Net Security, Stephen Cavey, Chief Evangelist at Ground Labs, talks about how businesses and job seekers are not only prioritizing data privacy but using it as a competitive advantage in this rivalrous landscape.

The challenges and advantages of building behavior-based threat detection

In this video for Help Net Security, Scott Sutherland, Senior Director, Adversary Simulation and Infrastructure Testing, NetSPI, discusses how, in order to stay ahead of malicious actors, organizations must shift their gaze to detect attackers before something bad happens.

Photos: Cyber Week 2022

Cyber Week is a large annual international cybersecurity event, hosted each year at Tel Aviv University in Israel. Cyber Week 2022 is held jointly by the Blavatnik Interdisciplinary Cyber Research Center (ICRC), The Yuval Ne'eman Workshop for Science, Technology and Security, Tel Aviv University, the Israeli National Cyber Directorate under the Prime Minister's Office and the Ministry of Foreign Affairs.

Cyber Week 2022 video walkthrough

In this Help Net Security video, we take you inside Cyber Week 2022. The featured vendors are: Dig Security, Ermetic, enso, Forescout, Flow, IBM Security, Intuit, Israel Aerospace Industries, Mitiga, and Synopsys.

Product showcase: Group-IB Unified Risk Platform

Group-IB has developed the Unified Risk Platform, a comprehensive set of solutions that understands each organization's threat profile and configures defenses, and responds to threats in real-time.

New infosec products of the week: July 1, 2022

Here's a look at the most interesting products from the past week, featuring releases from Fusion Risk Management, G-Core Labs, Rafay Systems, and RangeForce.

Infosec products of the month: June 2022

Here's a look at the most interesting products from the past month, featuring releases from: Acronis, Arcserve, Black Kite, Cavelo, Code42, ComplyCube, Cynet, Elastic, ESET, Feroot, Fusion Risk Management, G-Core Labs, Hillstone Networks, Incognia, Living Security, Lumu, NetWitness, Optiv Security, Qualys, Rafay Systems, RangeForce, SafeBreach, SecureAuth, SecurityMetrics, Splunk, Swimlane, and Traceable AI.

Cyber Week
June 27th-30th, 2022
Tel Aviv University, Israel
Yuval Ne'eman Workshop for Science, Technology and Security Tel Aviv University
ICRC Blavatnik Interdisciplinary Cyber Research Center
TEL AVIV UNIVERSITY אוניברסיטת תל אביב
Cyber Israel National Cyber Directorate
In cooperation with:
Ministry of Foreign Affairs Israel
ISRAEL CYBER ALLIANCE
State of Israel Ministry of Economy and Industry Foreign Trade Administration
ISRAEL EXPORT INSTITUTE

cybernews

Gathering storm: ransom gangs had over 700 victims last quarter

Kristina Jarusevičiūtė

The ransomware industry had some downs during the 2nd quarter of 2022, but even the fall of Conti, one of the most nefarious gangs out there, was not a setback for threat actor groups.

"Even with a war raging in Ukraine – the biggest global cyber threat we still face is ransomware," Lindy Cameron, the CEO of the National Cyber Security Center, said during her speech at Tel Aviv Cyber week.

Increase or a decline?

A recent report by cybersecurity company Cyberint showed an approximate 10% decrease in attacks across all ransomware groups compared to the 1st quarter.

However, threat intelligence firm Digital Shadows stated that the attack count increased by 21%.

While the results differ, senior analysts of both companies recorded a similar number of attacks during the quarter. Cyberint identified 709 victims, while Digital Shadows – 705.

In fact, Cyberint is far from being the first one to report a decline in ransomware. In May, Rob Joyce, the director of cybersecurity at the National Security Agency (NSA), said that the number of ransomware attacks plummeted due to sanctions against Russia.

Cyber insurers might have felt a temporary decline, too. Despite the disagreement over numbers, ransomware makes up for 10% of all breaches and has more than doubled in 2021.

Needless to say, the industry is not backing down, especially with veteran gangs upgrading and new groups joining.

The fall of Conti

The highlight of this quarter was the fall of Conti and its last kicks. "The most significant ransomware incident was performed by the Conti ransomware group. The attack took place in Costa Rica, started in April, and lasted for several weeks," the senior analysts of Cyberint told Cybernews. They also noted that this was the first time a ransomware group disrupted and affected residents and the government daily for a few months.

However, after Conti made the headlines back in February when its files were leaked to the public by a Ukrainian researcher, it took a toll on the ransomware group's activities.

"After a significant Q1, being only second to LockBit while infecting 127 victims, the group dropped to fourth place in victim count as they had only 45 victims in Q2, as the last victim was in May," Cyberint's senior analysts revealed.

Conti shut down its operations at the end of May and its data leak site at the end of June. Cyberint's analysts say it may not be over: "Ransomware groups work as agile units and keep rotating every once in a while; the death of Conti could only be the rebirth of multiple new sub-groups, which will deploy new techniques and procedures for gaining new victims."

New beginnings

While Conti retires, one of its biggest competitors, LockBit, introduces a revamped operation called "LockBit 3.0" that involves a bug bounty program. As the Cyberint report notes, although the group did not have as many victims as seen in the 1st quarter of 2022, it is still the ransomware market-leading gang.

Second after LockBit in terms of ransomware activities is BlackCat – a ransomware gang that is a rebrand of the DarkSide/BlackMatter groups. The execution of their attacks differs based on the gang members that deploy it, but the end goal to extort data is the same. The history of DarkSide/BlackMatter and their shutdowns after attacking critical infrastructures gives food for thought about whether history is going to repeat itself.

Additionally, the Karakurt ransomware group launched an onion-based leaking platform. Cyberint's data revealed that it currently holds 34 victims. The report states that if the gang's activities continue at the same rate as during this quarter, they may become "one of the rising threats" of the upcoming quarter.

What's next

Although the 2nd quarter showed a small decrease in ransomware gang attacks, it is not a pass to let guards down. The market is also introducing newcomers, such as Black Basta, which attacked at least 26 victims within one month of its emergence. Industry Spy also introduced a data extortion marketplace and later launched its ransomware operations.

While the fall of Conti is significant, considering they were the 4th most active group during this period according to Cyberint's data, the comeback of Karakurt and LockBit's upgrade does not signify a next quarter attack decrease.

Cyberint researchers do not believe that the ransomware gang era is nearing the end. It is more likely that groups spent this quarter developing their infrastructure, making the 2nd quarter of this year only a pre-storm period.

Cyber Week
June 27th-30th, 2022
Tel Aviv University, Israel
Yuval Ne'eman Workshop for Science, Technology and Security Tel Aviv University
ICRC Blavatnik Interdisciplinary Cyber Research Center
TEL AVIV UNIVERSITY אוניברסיטת תל אביב
Cyber Israel National Cyber Directorate
In cooperation with:
Ministry of Foreign Affairs Israel
ISRAEL CYBER ALLIANCE
State of Israel Ministry of Economy and Industry Foreign Trade Administration
ISRAEL EXPORT INSTITUTE

cybernews

In space, cutting losses invite cyberattacks

Vilius Petkauskas

The cybersecurity of commercial satellites can be on par with any government spacecraft. However, companies avoiding loss at all costs is precisely what ransomware gangs prey on. Besides, businesses don't shoot back.

The government monopoly in space has come to an end. Elon Musk's SpaceX alone runs over a third of all operational satellites currently in orbit. Having launched over two thousand spacecraft, the company plans to launch thousands more.

To keep up the pace, commercial satellites use more open-source software and hardware. While helping to cut costs, this could leave spacecraft more vulnerable to cyberattacks. However, Isaac Ben Israel, chairman of the Israeli Space Agency (ISA), thinks that commercial players do not leave space less secure for national space agencies.

Neither commercial satellites nor government-run satellites are immune to hacking, Major General (Ret) Israel thinks. Days of tailor-made hardware are long gone. Ransomware gangs and people defending against them often use the same tools. The same vulnerabilities apply, whether it's a company or a space agency.

"I think it's wrong to believe that safety was better just because few space organizations used to build satellites,"

Isaac Ben Israel, chairman of the Israeli Space Agency told Cybernews.

However, the critical difference in security lies not with the technology but with the mindset. Businesses are much more willing to pay up to cut their losses. Meanwhile, governments opt to retaliate instead of caving, an attitude that is inimical to crooks scouting for easy money.

We sat down with Major General (Ret), a key speaker in this years Cyber Week conference, Israel to discuss the effect commercial companies can have on space security, whether space agencies perceive cyberthreats as real, and if it's possible to avoid the militarization of space.

Commercial satellite makers rely on open-source software. At the same time, security regulations on satellite supply chains are only in the developing stage at best. Do you think the entry of companies to the space domain is leaving satellite infrastructure less secure?

The risks exist because communication depends on computers, not because commercial companies are involved. It doesn't matter whether the satellite is based on open-source or not. Hackers generally can hack into almost anything they like. Yes, it takes effort sometimes, and they don't always want to spend too much time doing it.

Sometimes bad actors don't have the resources to carry out the attack, but in principle, there is no big difference between private and government-owned satellites. If you'd like to hack into defense satellite communication, you can do it. The real question is about the volume of activity, which is increasing because the commercial world is joining in.

With an increasing number of satellites, there's more communication in space. And that increases the vulnerability of the system. But not because it's commercial. Private businesses can defend themselves the same way as defense or other organizations.

Some older satellite systems were hand-made for specific missions, while many nanosatellites rely on off-the-shelf materials. Don't you think that impacts the cyber safety of spacecraft?

I think it's wrong to believe that safety was better just because few space organizations used to build satellites. Maybe it was different because NASA or the Soviets secretly crafted satellites. However, now neither NASA nor the Israeli Space Agency makes parts, such as microchips, themselves.

For the past three decades, everyone has been using very similar devices. If you want to attack a space asset through the communication between the asset and the ground station, it's via the same computers. The ground stations that a threat actor may attack to influence the satellite in space are using the same computers, software, and hardware as anyone else. It's not hand-made. So, it doesn't matter if it's commercial or not.

And this phenomenon is very typical to cybersecurity, not only in space. The number of devices on Earth is increasing very fast. Computers became cheaper, more capable, smaller, and we put them in places [where] they did not exist two years ago. We have become dependent on computers in hospitals as much as in space.

Security experts discuss how financially motivated threat actors could use cyber means to hack satellites for

ransom. At ISA do you see hacker attacks as a real, contemporary threat?

Yes, it's a real threat. Not for the future, either. It has been like this for a decade. It's not that people don't know how to do it, but so far, there has been no interest in doing it. I think there is a difference between government-owned and private satellites, at least in one aspect. The chance that a government will agree to pay the ransom is minimal. Governments do not like to do it.

If it's a commercial entity, the equation is 'how much we earn' versus 'how much will we lose by paying.' Usually, hackers don't ask for much money, and companies opt to cut their losses. In this sense, there might be an indirect link between the level of safety and the number of commercial satellites. The more commercial space is, the more place there is for doing whatever is done to, for example, hospitals.

Another thing is that a government, unlike a business, may attack you back. And nobody wants that. Criminals want easy money and not to become a target for the United States government.

"A government, unlike a business, may attack you back. And nobody wants that. Criminals want easy money and not to become a target for the United States government,"

Major General (Ret) Israel thinks.

There's a strong sentiment that nation-states should avoid the militarization of space. Do you think it is possible to prevent space from becoming just another theater of war in the 21st century?

It's a matter of choice. You see, space is unique. It is the only place that so far was not militarized. If someone sent forces to a sovereign nation, its citizens would do whatever it took to fight back. That applies to land, air, and sea up to a certain distance. Space is the only exception.

There were some attempts to do that in the past. Advisors to the US President Ronald Reagan offered to weaponize space in the '80s. The media called it the Star Wars program. It was the peak of the Cold War, and the whole issue was about nuclear weapons. The idea was to put weapons in space to intercept missiles coming to the US.

The program didn't materialize, and space was kept as a kind of an extra-territorial, non-militarized, non-weaponized medium. This proves avoiding militarization is possible. However, whether it will remain like that mostly depends on what the US, Russia, and China will do.

Recent events in Ukraine have shown that services commercial space companies provide can be used in an active conflict. What lessons will national space agencies and militaries learn from this?

I think there are more general lessons about his conflict that apply not only in space but to the cybersecurity realm in general. The first question we have to ask ourselves is why nothing serious happened within the cyber domain. Knowing Russia's cyber capabilities, everybody expected a lot more. When historians write about this war 20 years from now, they will barely mention the cyber dimension.

There are many possible ways to answer this. Some people say the Russians were not interested in doing too much, so they wouldn't give the West an opportunity to hit back. However, that doesn't explain why they didn't use malware in Ukraine on a scale that was expected.

I think that you have to build the capability with any weapon, be it a tank, an aircraft, or a cyber weapon. You don't know when and where you will use it. It might be that you build a particular weapon, and the need to use it will come years later. And when the time comes, you find that the weapon doesn't fit you anymore.

The problem is that the timescale to build capability for hard weapons is 10-15 years. However, it may take months to keep the capability alive for a cyber weapon. You have to invest a lot more than in other areas. The Russians didn't do it. They built certain capabilities that they demonstrated in December 2015 by shutting off the power in western Ukraine for 24 hours.

The problem is that if you want to do something like this, you need to constantly check, for example, what software your adversaries are using. It takes a lot of time and energy because the rate of change here is very fast.

You cannot use cyber weapons in the same way you use aircraft. The typical time is too short. And that's why it was used only at the beginning of the war. It's possible to prepare specific capabilities for the start of the conflict. But only that. Contrary to what many say, I think this is the biggest lesson I would take from this war.

ComputerWeekly.com

Commercial cyber products must be used responsibly, says NCSC CEO

NCSC's Lindy Cameron is to speak out on responsible regulation of cyber capabilities at an event in Tel Aviv, Israel

Alex Scroxton

Tech companies that develop sophisticated cyber capabilities that could be co-opted by malicious actors have a responsibility to see that their sale is controlled and that they are used safely, National Cyber Security Centre (NCSC) CEO Lindy Cameron will tell an audience at Tel Aviv University's annual Cyber Week later today (28 June).

Calling for cooperation between institutions, technology companies and governments, Cameron will say: "If we're going to maintain a cyber space which is a safe and prosperous place for everyone, it is vital that such capabilities are produced and used in a way that is legal, responsible and proportionate."

Although it does not reference the events directly, Cameron's speech comes almost a year after the already-controversial Israel-based malware developer NSO Group became embroiled in a surveillance scandal after an investigative consortium revealed that its mobile remote access trojan (RAT), Pegasus, had been sold to repressive regimes that used it to spy on targets in other countries, including the UK.

The Pegasus RAT was linked to the murder of journalist Jamal Khashoggi by the Saudi Arabian authorities, among other things.

NSO Group has subsequently become the subject of restrictions and lawsuits in a number of jurisdictions, and at the end of 2021, the Israeli Ministries of Defence and Foreign Affairs tightened the country's export control rules for cyber technologies, although they made no mention of NSO Group as they did so.

"I am delighted that Israel has tightened export controls around these tools, making it far more difficult for nations with concerning records on privacy and human rights to acquire such intrusive spyware." Cameron will say.

"It is important that every actor, from the developer to the end-user of these types of technology and capability acts responsibly, with appropriate safeguards to protect against misuse."

Going forward, countries interested in acquiring a cyber or intelligence system from an Israeli company are obliged to sign an updated declaration as a condition for issuing an export licence, stating that its use will be restricted to the investigation and prevention of crime and terrorism. Note that this may not have prevented the sale of NSO's Pegasus malware in some circumstances, as the company has always maintained that it is sold for exactly that purpose.

Cameron will go on to describe Israel as a "shining example" of a state that takes cyber security seriously. "The technology developed here is truly world class," she will say. "The talent in the cyber security sector is second to none. And your defences are some of the strongest in the world.

"But making the most of our digital future is too big an issue for any one nation to handle alone. From drip-feed irrigation to dramatic medical advances, Israel has always proudly innovated for the benefit of people well beyond your borders. So I hope you will continue to produce cyber security solutions which are safe, strong, but also affordable for the whole world.

"To succeed, partnerships are essential. So, we are building stronger ties between academia, industry and government. We must come together around our shared values, each nation bringing its own particular skills and strengths to build a network that is naturally resilient to attack, one that favours innovation, discourse and creativity over control and coercion."

Cameron's speech will also touch on the current threat landscape, noting that even with the cyber element of Russia's illegal invasion of Ukraine, it is ransomware that remains the most pressing security threat.

"Just as they have on the battlefield, the Ukrainian cyber defenders have done an incredible job of repelling many of these attacks," she will say. "They are real heroes. Resilience and preparation is at the heart of this success.

"But even with a war raging in Ukraine, the biggest global cyber threat most organisations face is still ransomware. That tells you something of the scale of the problem.

"Ransomware attacks strike hard and fast. They are evolving rapidly, are all-pervasive, and are increasingly offered by gangs as a service, lowering the bar for entry into cyber crime. And it is this that makes them such a pernicious threat – not just the nationally significant incidents we deal with in NCSC, but also the hundreds of incidents we see nationwide every year.

"These complex attacks have the potential to affect our societies and economies significantly, were it not for the expertise of our incident management operators working in collaboration with their counterparts in industry and international governments."

ZDNet

Ransomware is the biggest global cyber threat. And the attacks are still evolving

Ransomware attacks 'strike hard and fast', warns NCSC chief.
Danny Palmer

Ransomware is the biggest cybersecurity threat facing the world today, with the potential to significantly affect whole societies and economies – and the attacks are unrelenting, the head of the National Cyber Security Centre (NCSC) has warned.

"Even with a war raging in Ukraine – the biggest global cyber threat we still face is ransomware. That tells you something of the scale of the problem. Ransomware attacks strike hard and fast. They are evolving rapidly, they are all-pervasive, they're increasingly offered by gangs as a service, lowering the bar for entry into cyber crime," said Lindy Cameron, CEO of the NCSC In a speech at Tel Aviv Cyber Week.

While she didn't detail any specific instances of responding to ransomware incidents, Cameron warned that "these complex attacks have the potential to affect our societies and economies significantly", and implied that if it weren't for the work of NCSC incident responders, alongside their counterparts in the industry and international counterparts, the attacks could have had a major impact.

Working alongside other law enforcement agencies, Cameron said that the NCSC is working to understand the criminal system that helps drive ransomware attacks – and how the nature of ransomware gangs and the techniques they're using to facilitate ransomware campaigns continue to evolve.

"We want to make ransomware an unprofitable and unattractive business," said Cameron, who argued it's not all doom and gloom when it comes to cybersecurity, going on to detail how the NCSC's Active Cyber Defence Program has helped to disrupt cyberattacks targeting citizens.

This includes a takedown project that has removed millions of malicious URLs, and the suspicious email-reporting service, which has allowed the public to report over 10.5 million suspicious emails, leading to over 76,000 online scams being taken down.

"We want to help create a society that is resilient to cyberattacks, where cybersecurity is second nature to all of us," said Cameron.

According to newly released figures from cybersecurity company WatchGuard, the volume of ransomware has risen significantly with the amount of detected activity in the first quarter of 2022 more than three times what was detected during the same period last year.

The report suggests that the emergence of aggressive ransomware and extortion operations including LAPSUS$ and BlackCat are behind what's described as "an ever-increasing ransomware and cyber-extortion threat landscape."

Geektime

The War in Ukraine: Important lessons to be learnt from Ukraine's cyber defence success

Ukraine managed to thwart many Russian-sponsored cyber-attacks prior to and during the war. What lessons can states learn and apply?

As you read this, Israel's annual Cyber Week, the leading international cybersecurity event where experts from around the world share their knowledge on the challenges and opportunities in the field, is taking place. Omree Wechsler, a senior researcher on cyber security and featured speaker at the conference shared his insights regarding the current Ukrainian war.

With the amassing of Russian forces on Ukraine's borders in January and February 2022, many observers believed that the world is about to witness the first cyber war. Given that Russia ranks very high in terms of offensive cyber capabilities, and that many Ukrainian infrastructures are built on Russian software and hardware, many believed that Russia would paralyze and knock off Ukrainian critical infrastructure and services. Despite the predictions, the Russian war effort was not accompanied by any successful major cyber blows to Ukrainian critical infrastructure, and its distributed denial of service (DDoS) and wiper attacks failed at large to curb Ukraine's ability to defend itself.

Alongside the partial results of its cyber warfare efforts, even greater failures plagued the performance of the Russian armed forces on the physical battlefield. If anything, the war has demonstrated the severe challenges facing an invading army attempting to overcome fierce resistance that enjoys international support. Before the invasion, many observers warned that any Russian success would encourage other states to pursue their geopolitical goals with military means. However, given these difficulties, states are unlikely to resort more to military invasions and are more likely to continue to develop gray-zone warfare tactics, including cyberattacks and disinformation campaigns.

Current and future risks of cyberattacks and information warfare necessitate the understanding and applying of lessons from Ukraine. While the perceived failure of the Russian cyber effort is also rooted in internal Russian gaps and challenges, it is crucial to look at the lessons from Ukraine's perspective. First, it is wise to take notes of years of preparations made by Ukraine. These efforts revolve around common measures that are relevant for states as well as organizations and may sometimes be neglected due to budgetary or organizational issues. According to Viktor Zhora, Deputy Chair of the State Service of Special Communications and Information Protection, Ukraine has moved to tackle challenges such as the widespread use of old and sometimes, unlicensed software, which has raised the awareness amongst operators of critical infrastructure and has connected them to Security Operations Centers (SOC) to quickly detect and respond to cyber incidents. Moreover, the country has established new facilities to conduct cyber defence exercises and simulate attacks.

Second, much of Ukraine's ability to thwart Russian cyberattacks could be attributed to the heavy technical assistance the country has received from its allies, headed by the U.S., since the infamous BlackEnergy cyberattack

that had targeted its power grid in 2015. In recent years, the U.S. Cyber Command has been sending teams to Ukraine as part of the so-called "Hunt Forward" operations. These teams, many of which arrived in Ukraine around October 2021, helped to detect, and clean up a so-called "wiper" malware – one that deletes files that are crucial for the operation of systems from the national railway systems.

The third lesson is about maintaining redundancy. Just hours before the invasion on February 24, Russia successfully knocked off satellite communications connectivity provided by the American satellite company Viasat, which was used by the Ukrainian military to communicate with front-line troops. However, internet connectivity was quickly regained as SpaceX's Starlink system terminals started arriving in Ukraine at the request of the country's deputy prime minister, Mykhailo Fedorov.

A fourth lesson should focus on Ukraine's success in defending against Russian information warfare and in gaining supremacy in the information domain. Crucial to increase morale, maintain internal unity, and receive international support, Ukraine has managed to control strategic narratives and fully capture the media space via social media channels etc. Gaining an advantage in information warfare requires an understanding of the opponent's methods and modus operandi and acting proactively. Ukraine's success could be attributed to familiarity with Russian (or Soviet) tactics and the fact that the country has been struggling with hybrid warfare and disinformation campaigns at least since the annexation of Crimea in 2014.

Some countries, such as China and Iran have been learning and incorporating the Russian playbook into their own tactics. In October 2019, Cyber Command and NSA's director, General Paul Nakasone pointed out Chinese efforts to subvert pro-democratic demonstrations in Hong Kong with a social media disinformation campaign. Iranian hackers stole the personal information of American voters prior to the 2020 presidential elections and used it to intimidate voters and spread false information regarding electoral frauds.

While many political, cultural, and contextual differences exist between states, there are many lessons to be learnt from Ukraine's success in fending off Russia's cyberwarfare efforts that could be applied around the world.

Written by Omree Wechsler, a senior researcher at the Blavantnik Interdisciplinary Cyber Research Center, Tel Aviv University

CTECH

The cyber arena is "more significant than ever," says Team8

The summit will be attended by more than 100 CISOs from leading companies like Intuit, MasterCard, and Walmart and coincide with the start of Tel Aviv University's Cyber Week
James Spiro

"In recent weeks we have witnessed significant changes, characterized by de-globalization and economic slowdown, which are dramatically affecting the world, and may also directly impact the frequency of cyberattacks, making the cyber arena more significant than ever," said Team8 Managing Partner Nadav Zafrir.

Zafrir made the comments ahead of the first day of the CISO Summit, a global cybersecurity summit hosted by Israeli venture capital firm Team8. The summit brings together experts who will discuss the future of cybersecurity with an emphasis on challenges and opportunities.

"At Team8 we have identified a real need to bring together the best cyber experts in the world, including 100 CISOs from well-known companies, and thought leaders from the Israeli cyber industry for five full days of in-depth discussions," he continued. "Together, we will be better equipped to understand our challenges and opportunities, and better positioned to plan accordingly."

The five-day summit began today and will include in-depth discussions from CISOs at companies such as Walmart, Unilever, GM Financial, Intuit, MasterCard, and more. During their stay in Israel, they will interact with local startups such as Claroty, Sygnia, Talon, Akeyless, Illusive, Cyberpion, Silverfort, Authomize, Cardinal, Orca Security, Ermetic, SafeBreach, and Resilion.

Among the topics to be discussed include the shifting approaches to attackers and attack strategies and the impact of economic and geopolitical changes on the cybersecurity industry across domains such as cloud security, 5G, privacy, and regulation.

The closing of the event will coincide with the official opening event of Tel Aviv University's Israeli Cyber Week, which is scheduled to take place from June 27-30. It will be co-hosted by Team8 with sponsorship from industry partners including Deloitte, Leumi-Tech, Meitar Law Office, Valley Bank, Palo Alto, FinSec - Mastercard, and Enel's Innovation Lab. It is expected to include speakers such as Renee Wynn, Former NASA Chief Information Officer; Admiral Mike Rogers, former director of the NSA and Operating Partner at Team8; Nadav Zafrir, former 8200 unit commander and Managing Partner at Team8; and Nir Minerbi, CEO and Co-Founder of quantum computing startup, Classiq.

CTECH

"Quantum computing will revolutionize every large industry"

Nir Minerbi, Co-founder and CEO of Classiq, was speaking during an event organized by Team8 to kick off Cyber Week
James Spiro

Israeli Team8 venture group officially opened this year's Cyber Week with an event that took place in Tel Aviv on Sunday. The event, which included international guests and cybersecurity professionals, showcased the country and the industry as a powerhouse in relation to Startup Nation.

Opening remarks were made by Niv Sultan, star of Apple TV's 'Tehran', who also moderated the event. She then welcomed Gili Drob-Heinstein, Executive Director at the Blavatnik Interdisciplinary Cyber Research Center (ICRC) at Tel Aviv University, and Nadav Zafrir, Co-founder of Team8 and Managing Partner of Team8 Platform to the stage.

"I would like to thank the 100 CSOs who came to stay with us," Zafrir said on stage. Guests from around the world had flown into Israel and spent time connecting with one another ahead of the official start of Cyber Week on Monday. Team8 was also celebrating its 8th year as a VC, highlighting the work it has done in the cybersecurity arena.

The stage was then filled with Admiral Mike Rogers and Nir Minerbi, Co-founder and CEO of Classiq, who together discussed 'The Quantum Opportunity' in computing. "Classical computers are great, but for some of the most complex challenges humanity is facing, they are not suitable," said Minerbi. "Quantum computing will revolutionize every large industry."

Classiq develops software for quantum algorithms. Founded in 2020, it has raised a total of $51 million and is funded by Team8 among other VC players in the space. Admiral Mike Rogers is the Former Director of American agency the NSA and is an Operating Partner at Team8.

"We are in a race," Rogers told the large crowd. "This is a technology believed to have advantages for our daily lives and national security. I told both presidents I worked under why they should invest billions into quantum," citing the ability to look at multiple qubits simultaneously thus speeding up the ability to process information. According to Rogers, governments have already publicly announced $29 billion of funding to help develop quantum computing.

Final remarks were made by Renee Wynn, former CIO at NASA, who discussed the potential of cyber in space. "Space may be the final frontier, and if we do not do anything else than what we are doing now, it will be chaos 100 miles above your head," she warned. On stage, she spoke to the audience about the threats in space and how satellites could be hijacked for nefarious reasons.

"Cybersecurity and satellites are so important," she concluded. "Let's bring the space teams together with the cybersecurity teams and help save lives."

After the remarks, the stage was then transformed to host the evening's entertainment. Israeli-American puppet band Red Band performed a variety of songs and was then joined by Marina Maximilian, an Israeli singer-songwriter and actress, who shared the stage with the colorful puppets.

The event was sponsored by Meitar, Delloitte, LeumiTech, Valley, Palo Alto, FinSec Innovation Lab, and SentinelOne. It marked the beginning of Cyber Week, a three-day conference hosted by Tel Aviv University that will welcome a variety of cybersecurity professionals for workshops, networking opportunities, and panel discussions. It is understood that this year will have 9,000 attendees, 400 speakers, and host people from 80 different countries.

Cyber Week
June 27th-30th, 2022
Tel Aviv University, Israel
Yuval Ne'eman Workshop for Science, Technology and Security Tel Aviv University
Blavatnik Interdisciplinary Cyber Research Center
TEL AVIV UNIVERSITY אוניברסיטת תל אביב
Cyber Israel National Cyber Directorate
In cooperation with:
Ministry of Foreign Affairs Israel
ISRAEL CYBER ALLIANCE
State of Israel Ministry of Economy and Industry Foreign Trade Administration
ISRAEL EXPORT INSTITUTE

CTECH

The internet is "at risk of fracturing" amid geopolitical unrest and unregulated tech companies

Technology is both the underlying problem and solution to the world's biggest challenges off and on the internet, explains Dr. Melanie Garson of the Tony Blair Institute for Global Change
James Spiro

Dr. Melanie Garson of the Tony Blair Institute for Global Change

When the internet was created, its creators, full of idealism and optimism, imagined an open place that would improve communication and encourage education. It would connect like-minded strangers to one another who otherwise would never have met. It would shrink the distance between us while enlarging our exposure to different ideas and cultures.

As time went on, it also became clear that the internet would grow larger than anyone could anticipate - and with that, bring with it a slew of criminality and national security risks. To some, it would endanger free speech rights, to others, it would destroy democratic foundations in elections. Today, it runs the risk of becoming a 'splinternet' that breaks off into different economic, technological, and commercial factions run by nations or private companies.

"I think of an internet ecosystem, it is not just 'the internet'," explained Dr. Melanie Garson, the Policy Lead for Europe, Israel, and the Middle East in the Internet Policy Unit at the Tony Blair Institute for Global Change. "If we are looking at this from a geopolitical national security standpoint, it is literally everything from the submarine cables to the satellite system that is helping run it. Anything that creates a structure for the internet to run - and everything running on it... It is constantly expanding, it's like it's breathing."

Dr. Garson joined CTech during her visit to Israel for Cyber Week to discuss some of the biggest threats faced by nations and governments in an age where conflict, and potentially warfare, can be conducted solely on the internet. In her role at the TBI, she communicates with advisory teams who speak to governments and think tanks about cyber, tech, and foreign policy and how countries can work on their cyber capacity building, implement tech and innovation policies, and focus on safe data governance. Regarding tech companies, her team examines their responsibilities and their geopolitical actions.

The job encompassed a variety of roles and duties regarding a myriad of sections. She described it as "dealing with some of the endemic problems that are splintering or challenging the use of the internet."

"While we see it as a living breathing organism that is constantly in this exponential phase of growth, at the moment it is at risk of being splintered," she continued. "There is talk about the splinternet where we are getting the internet dividing along different ideological lines."

What does that look like, exactly? Dr. Garson highlights the work of Wendy Hall, who has suggested that the internet could in theory split into four ideologies: "The Silicon Valley Open Internet, the Brussels Bourgeois Internet, the DC Commercial Internet, and the Beijing Paternal Internet." Other examples are that nations could take care of their own internet structures by controlling the stream of information and communication they give to their citizens. The repercussions of this can lead to a weakening of the internet as a whole, making it easier for bad actors to lead attacks on businesses and governments.

At the start of the Russia/Ukraine crisis, Ukrainian Minister of Digital Transformation Mykhailo Fedorov suggested that the world 'cuts Russia off' of the internet - the ultimate sanction that would impact its citizens as much as traditional trade sanctions from foreign nations. While the internet standards organization IETF (Internet Engineering Task Force) and Internet Governance Forum (IGF) refused, it didn't prevent private companies like Apple, Meta, Google, and others from stopping or curbing their operations there.

"Tech companies need to work on thinking together about their deliberation process for their choices in this geopolitical intervention, to make sure they have consistency," Dr. Garson warned. "This time they happen to feel they are on the right side of history. But what happens when it is slightly not as clear cut?"

The internet can be used by companies to implement crippling social and economic sanctions, and it can also be used to bring governments down. The world has never been more connected, and as a consequence has never been so prone to cyberattacks. TBI works with governments to help them protect their critical infrastructure from attacks. One story that has strangely avoided the news cycles is how the Costa Rican government has been held at ransom for the last few months by crippling the country's essential services - with hackers demanding a $20 million payout. The conflict is still ongoing.

"We are getting that nexus from where cyber becomes not just criminal but also politically extraordinarily

dangerous," she continued. "It is a huge case for not just about making sure we get our key technologies secure, it is not just about critical infrastructure, which is where everyone has their shields up at the moment, but thinking about your political system. It's not just bots coming from Russia and China telling people how to vote, this is something quite insidious, which is something people should be prepared for."

The effort to make governments better protected against cyberattacks must be an equal one, or it results in lower-income countries becoming easy targets for hackers. "They're not quite attuned to the geopolitical arguments... where they sit on the geopolitical argument doesn't make them feel they're at threat," Dr. Garson explained, regarding countries and their position relative to conflicts such as Russia and Ukraine. "These lower-middle-income countries that aren't investing in their cybersecurity become the low-hanging fruit. It is much easier to go and be a pickpocket than rob a bank."

And so, as the internet risks splintering into different fractions, it runs the risk of hurting poorer countries, emboldening unregulated tech companies, and distorting the world's new infrastructure. Dr. Garson has conceded that governments have already shown two faults that dispel any cyber World War narratives: limitations of cyber as a tool in active conflicts, and limitations on governments to be agile enough to strengthen the internet ecosystem. The void is filled by tech companies that have "critical roles" in conflicts going forward.

"As an institute, we are very much tech optimists. We very much believe in the power of tech to have a radical difference in people's lives for the better. And that's the endgame - how can we harness these technologies to really improve people's lives more quickly, and the challenge we think about particularly for tech companies to build in some of these checks and balances... most technology companies, I tend to believe, are idealists," she concluded.

CTECH

Rethinking organizational cybersecurity strategy for corporations

"The fact that commercial companies have experienced such attacks casts doubt on the assumption that they don't need to include nation state level attacks as one of the threats to be addressed," writes Dr. Yaniv Harel, CSO at the Blavantnik Interdisciplinary Cyber Research Center

Yaniv Harel

Yaniv Harel

A nation state actor is characterized by the ability to focus on a single target in a way that doesn't correlate with the financial benefit of the attack, to plan a complicated sequence of actions, and to use unique and destructive types of malwares. Such actors typically have a backend operation equipped with advanced control capabilities, moreover, they support their activities with various intelligence sources.

Cybercrime attack groups continuously get more sophisticated and much more business oriented. In most cases, their activities are planned, and their efforts are invested in correlation with potential financial gains. It has been observed that attack actors may abandon a target, even one in which they have invested significant effort once they cross a predefined threshold beyond which the potential gains cannot be justified. They may leave a ransomware negotiation if they realize that the potential target won't pay.

It is common to divide threat actors into three groups - individual attackers, cybercrime groups, and nation state attackers. These days, organizations around the world allocate many millions to cybersecurity, with budgets reaching tens and even hundreds of millions of dollars in large enterprises. As part of the budget plan, organizations identify their priorities and the solutions chosen to protect themselves against the defined risks. A critical infrastructure company, for example, would put a different set of solutions in place than an educational institution.

Since the budget is finite, organizations should prioritize their investments, and many decide to exclude solutions for nation state attacks. As a security leader you have to decide what are the typical attacks that may challenge the organization and who are the most likely attackers that will choose the organization as a target. CISOs/CSOs are known to say: "If a nation decides to attack us – this is a scenario we are not going to cope with, and we have approved this with our Executive management". Statements such as this are made under

the assumption that solutions for nation-level threats are more complex and require a higher level of expertise.

There is also a common belief that national entities typically target governmental agencies and not private companies. These are their typical targets for intelligence collection purposes, and when escalated, their attack targets. This was true for many years in the intelligence and military arena. Nations follow other nations' data, and not commercial organizations' information.

In recent years, we have observed a change that should concern business entities. The supply chain attacks that started with SolarWinds have brought nation state methods into the business arena. The creation of complex infrastructure that enables access to companies via a legitimate platform and then selects them as targets for attack, is a significant state level approach. Therefore, it is not surprising that a few months later the Kaseya attack employed a similar technique, this time leveraging a managed security platform instead of an IT management platform.

Several specific cases that were exposed during the last few months describe dedicated efforts in which groups put a broad endeavor to build an infrastructure and to use strong components as the methodologies of nation state actors. In Praying Mantis for example, exposed by Signia's team, the attackers used Zero-day malware in a sophisticated way. Moreover, while they are aware of advanced monitoring and detection techniques, they developed sporadic command and control channels to the attack tools providing more resiliency against popular cybersecurity detection systems. A more local example is the POLONIUM case that Microsoft Threat Intelligence Center has exposed. The attack group used OneDrive and AirVPN as part of their attack channels. In one of the cases a cloud service provider was compromised. POLONIUM pivoted through the service provider and gained access to a law firm and an aviation company. In other cases, POLONIUM has been observed deploying a series of custom implants that utilize cloud services for command and control as well as data exfiltration.

The fact that commercial companies have experienced such attacks casts doubt on the assumption that they don't need to include nation state level attacks as one of the threats to be addressed. The question whether we are dealing with a nation state entity that targeted a commercial company, or a cybercrime organization that accomplished a nation-class attack array, is not important. What is significant is the conclusion that arises. The common assumption should be reconsidered, and different priorities and plans may emerge out of the new perspective.

Management teams and boards of directors should rethink the approved strategy that is the base for their cyber security organizational program. CISOs must revisit their resiliency programs, and insurance companies should evaluate the level of requirements they pose for large organizations.

This change shouldn't land only on the CISOs' tables. This assumption variation is a wake-up call for global governments as well. They should act at the legislation, enforcement, and collaboration levels that in the long term will help to prevent these types of attacks on top of expecting the companies to defend against them.

Dr. Yaniv Harel is the CSO at the Blavantnik Interdisciplinary Cyber Research Center

yahoo! finance

Israel's 12th Annual Cyber Week Highlights Unprecedented Changes in the Cyber Landscape and the Critical Need For Coordinated Response

TEL AVIV, Israel, June 29, 2022 /PRNewswire/ -- Top Israeli government figures such as Prime Minister Naftali Bennett and Defense Minister Benny Gantz, addressed the conference which is headed by Maj. Gen. (Ret.) Prof Isaac Ben-Israel, known as the "father" of the Israeli Cyber industry. Leading American and British cyber officials also contributed, including Chris Inglis the National Cyber Director at the Executive Office of the President at the White House, Anne Neurberger the Deputy Assistant to the US President and Deputy National Security Advisor for Cyber and Emerging Technologies at the White House, and Lindy Cameron CEO of the National Cyber Security Centre. Private sector leaders including Ira Winkler, Chief Security Officer for Walmart, Tim Brown CISO of SolarWinds, Jane Horvath, Chief Privacy Officer of Apple, Jason Chan, Former VP of Information Security at Netflix, also addressed the conference. Supported by Israel's Ministry of Economy and Innovation, attendees joined from over 80 countries from all over the world. Guests included startups and major investors, together with numerous sponsors, and partners.

Cyber Week is jointly held by the Blavatnik Interdisciplinary Cyber Research Center (ICRC); The Yuval Ne'eman Workshop for Science, Technology and Security at Tel Aviv University; and the Israeli National Cyber Directorate under the Prime Minister's Office. The gathering occurred against the backdrop of unprecedented cyber challenges and events including Russia's war on Ukraine. Speakers described a dramatic and concerning rise in cyber warfare as well as cybercrime - cyber-related damage is predicted to hit $10.5 trillion annually by 2025, while cybersecurity spending on data protection and risk management could reach $172 billion globally in 2022. Yet they also expressed hope in the effectiveness of properly implemented defenses and evolution in defensive cyber techniques to meet the challenge.

Israel's Prime Minister Naftali Bennett pointed out how "inevitably cyber is going to become one if not the most prominent dimensions of future warfare," while drawing attention to the vital need for global collaboration in the cyber sphere saying, "In cyber it's [collaboration] vital because the same bad guys who are attacking one company or country are attacking others at the same time. If you can share that information everyone else can defend themselves. It's like a pickpocket in a subway and if someone sprays them with red paint everyone can see and defend themselves."

Ira Winkler: CISSP, Chief Security Architect, Walmart outlined the important role government plays saying, "at a high level, governance tells people how to do things correctly with cyber security at the forefront." He also recognized the need to account for the human aspect of cyber and to be realistic when devising and implementing strategy, "A user is as much as part of the system as a computer. Stop expecting people not to

click on suspicious content, but rather have a strong network protecting them."

Israel's Minister of Defense, Benny Gantz, outlined the increasing shift of conflict to the cybersphere and that bad actors are already carrying out attacks via cyber, particularly Iran. The country uses "new [cyber] proxies [who] "are terrorists with keyboards," in addition to their direct actions. In response, Defense Minister Gantz stressed the need for private companies to follow government guidelines and cooperate saying, "Iran is first a global challenge, then it is a regional challenge, and only finally is it a threat to the State of Israel. The same goes for the cyber dimensions and the same framework of cooperation vis-a-vis Iran is expanding to cyber."

About CyberWeek:

Cyber Week is a leading international cybersecurity event that provides a unique opportunity for experts from industry, government, military and academia to share their knowledge about the challenges and opportunities in the field. Cyber Week is hosted by the Blavatnik Interdisciplinary Cyber Research Center and the Yuval Ne'eman Workshop for Science, Technology, and Security, at Tel Aviv University, headed by Major Gen. (Ret.) Prof. Isaac Ben-Israel together with the National Cyber Directorate at the Prime Minister's Office, The Ministry of Economy and Industry, and the Ministry of Foreign Affairs.

THE TIMES OF ISRAEL

Israel has drastically damaged Iran's intelligence operations, Iranian officials say

NYT: Israeli distrust-sowing moves see Revolutionary Guard intel chief ousted after foiled Turkey plot, senior officer nabbed; Israel 'infiltrated deep' into Iran security circles

Israel has deeply infiltrated and drastically shaken Iranian intelligence operations in recent months, a senior Iranian official told the New York Times.

The report published Wednesday cited the recent ousting of the intelligence chief of the Islamic Revolutionary Guard Corps and the secret arrest of a senior commander accused of spying for Israel as examples of the growing levels of distrust in Iran.

Mohammad Ali Abtahi, a former vice president of Iran who lives in Tehran and still maintains close ties with top officials, told the newspaper that Israeli operations had seriously damaged trust within the country's security establishment.

"The security breaches inside Iran and the vast scope of operations by Israel have really undermined our most powerful intelligence organization," he said.

"The strength of our security has always been the bedrock of the Islamic Republic and it has been damaged in the past year," Abtahi said, telling the newspaper that the Iranian defense establishment would now be looking for a new approach.

The report said that unnamed Iranian officials also admitted that "Israel's spy network has infiltrated deep into the rank and file of Iran's security circles."

Iranian Vice President Mohammad Ali Abtahi speaks with media as he leaves a cabinet meeting in this Sept. 17, 2003 file photo (AP Photo/Vahid Salemi, file)

Israel has allegedly stepped up its attacks on Iran's nuclear program in recent months.

Israeli officials told the Times that this was a deliberate tactic to expose failures by the IRGC, generating conflict between the political and defense establishments in Iran.

Iran's decision to replace the intelligence chief of the IRGC, Hossein Taeb, who had held the position for more than 12 years, was seen as a prime example of the long-running campaign by Israel.

The Times reported that Taeb had "seemed untouchable" before a number of recent high-profile killings blamed on Israel and before the apparently foiled Iranian plan to attack Israelis in Turkey.

An unnamed adviser to the Iranian government and an individual affiliated with the IRGC both told the newspaper that Taeb had been tasked with exposing Israel's spy network in Iran.

Israeli intelligence officials who requested anonymity told the newspaper that the thwarting by Israeli and Turkish security forces of the plot had proved the final straw for officials, who abruptly removed Taeb from his position.

But the report also said calls for Taeb to be ousted had already been voiced in the wake of increasing distrust among senior Iranian officials after a senior commander in the Revolutionary Guards, Brig. Gen. Ali Nasiri, was secretly arrested amid allegations that he spied for Israel.

Iranian officials with knowledge of Nasiri's detention said he was placed in custody earlier this month, around two months after a wave of arrests in which several dozen Iranian Defense Ministry employees were arrested on suspicion of leaking classified materials to Israel.

In this September 21, 2016, file photo, Iran's Revolutionary Guard troops march in a military parade in Tehran, Iran. (AP Photo/Ebrahim Noroozi, File)

Nasiri held a high-level position in the IRGC's Protection of Information Unit, a branch of the force responsible for supervising the Guard Corps' operations, the Times said.

His arrest had begun to rattle senior Iranian officials who already had concerns about Taeb, but the balance was tipped after Israel exposed the plot against its citizens in Turkey.

Jerusalem reportedly told Ankara that Taeb was behind the planned attacks.

Taeb was a trusted ally of Iranian Supreme Leader Ayatollah Ali Khamenei, and prior to his appointment in the IRGC was notorious for his role in brutal crackdowns on protestors.

Iran and Israel have been engaged in a years-long shadow war but tensions have ratcheted up following a string of high-profile incidents Tehran has blamed on Jerusalem.

A number of members of the IRGC and scientists have been killed in recent weeks, with Iran often pointing the finger at Israel.

Two Turkish riot police officers walk in front of the Blue Mosque in Istanbul, on June 14, 2022. (Yasin Akgul/AFP)

Iran reportedly suspects Israel killed two Iranian scientists several weeks ago by poisoning their food. The details of the men's work, the circumstances of their deaths and their ties to the government remain unclear.

On June 13, Ali Kamani, a member of the Guard's aerospace division, was killed while on a mission in Khomein in the central province of Markazi, the IRGC said in a statement, without elaborating.

Earlier in June, Colonel Ali Esmailzadeh, a commander of the IRGC's external operations unit, the Quds Force, died "in an accident in his home," according to state news agency IRNA.

And on May 22, Guards Colonel Hassan Sayyad Khodaei, 50, was killed outside his home in the east of the Iranian capital by attackers on motorbikes who shot him five times. State television in Iran said Khodaei was a member of the Quds Force and that he was "known" in Syria, where Iran has acknowledged deploying "military advisers."

The IRGC described Khodaei as a "defender of the sanctuary," a term used for those who work on behalf of the Islamic Republic in Syria or Iraq, accused "Zionists" of being behind the assassination, and vowed revenge.

People walk past a banner showing Iran's Revolutionary Guard Col. Hassan Sayyad Khodaei, prior to his funeral ceremony, in Tehran, Iran, May 24, 2022. (Vahid Salemi/AP)

And late last month, an engineer was killed and another employee injured in Iran's Parchin military complex under unclear circumstances. The New York Times reported that the deadly explosion at the military complex was caused by quadcopter suicide drones. Iran said the man was killed by "industrial sabotage."

There have also been a number of attacks — both physical and cyberattacks — on nuclear and industrial facilities in recent months.

Israel and Iran have for years been involved in a largely clandestine cyberwar that occasionally bubbles to the surface. Most recently, Iran's major steel companies were hit by a cyberattack on Monday.

Israeli military correspondents, who are regularly briefed off-the-record by senior Israeli officials, hinted that Israel was directly responsible for the assault in retaliation to a suspected cyberattack that caused rocket sirens to be heard in Jerusalem and Eilat last week.

Outgoing Prime Minister Naftali Bennett warned Tuesday that anyone who attempts a cyberattack against Israel will "pay a price."

"[The] approach with our enemies, especially Iran... we don't go around wreaking havoc in Tehran — that's never been our policy. Our policy is, if you mess with Israel, you'll pay a price," Bennett said at the Cyber Week conference in Tel Aviv.

THE TIMES OF ISRAEL

'Mess with Israel, you'll pay a price,' PM warns Iran, after steel plant cyberattack

At Cyber Week event, Bennett says 'wreaking havoc in Tehran' not a policy, but Israel will respond to assaults; 'smart folks' at keyboard can do what commandos do without the risks

EMANUEL FABIAN

Outgoing Prime Minister Naftali Bennett warned Tuesday, a day after Iran's major steel companies were hit by a cyberattack, that anyone who attempts a cyberattack against Israel will "pay a price."

"[The] approach with our enemies, especially Iran... we don't go around wreaking havoc in Tehran — that's never been our policy. Our policy is, if you mess with Israel, you'll pay a price," Bennett said at the Cyber Week conference in Tel Aviv.

He also highlighted the benefits of using cyber warfare over more traditional military offensive methods, noting, "You can get a bunch of smart folks sitting on a keyboard to achieve the same effect... without risking your soldiers' lives."

Monday's large cyberattack forced the state-owned Khuzestan Steel Co. to halt production, and two other major steel producers also reported being targeted.

An anonymous hacking group claimed responsibility on social media for the attack, saying it had targeted Iran's three biggest steel companies in response to the "aggression of the Islamic Republic."

The group, calling itself "Gonjeshke Darande," shared what purported to be closed-circuit footage from the Khuzestan Steel Co. factory floor that showed the malfunction of a piece of heavy machinery on a steel bar production line, causing a massive fire.

Israeli military correspondents, who are regularly briefed off-the-record by senior Israeli officials, hinted that Israel was directly responsible for the assault in retaliation to a suspected cyberattack that caused rocket sirens to be heard in Jerusalem and Eilat last week.

Bennett was asked at the conference about his approach as prime minister to cyber offense and defense, and gave a lengthy, considered response.

Prime Minister Naftali Bennett speaks with Michal Braverman-Blumenstyk, Microsoft corporate VP and CEO of the Israel R&D Center at the annual cybersecurity conference Cyber Week at Tel Aviv University, June 28, 2022. (Cyber Week, Tel Aviv University)

"Today you can get stuff done hitting your enemy through cyber which in the past would require to covertly send 50 or 100 commando soldiers behind enemy lines with huge risk," he said. "And now you can get a bunch of smart folks sitting on a keyboard to achieve the same effect. So it's a no-brainer. And this is why inevitably cyber is going to become one of, if not the most prominent dimensions of future warfare. It just makes sense... If you can get the same effect through cyber without risking your soldiers' lives, obviously it's going to happen."

"On the geopolitical level," Bennett added, "we're going to see a lot of investment across the world in cyber offense... It's only going to get worse, the threat... With critical infrastructure, we're doing pretty well on the defensive side and of course on the military dimensions of defending ourselves."

He said he was "a bit surprised" by the relative "lack of use of cyber tools in the war in Ukraine."

Bennett then specified his policies on cyberwarfare, particularly as related to Iran:

"Just like there's nuclear deterrence, there's going to be cyber deterrence," he said. "And my approach generally with our enemies, especially Iran, is, we don't go around just wreaking havoc in Tehran. That's never been our policy. Our policy is, though, that if you mess with Israel, you'll pay a price. And you can no longer hit Israel indirectly through proxies, through Hezbollah, through Hamas, and think you'll get away with it.

"If you're the bully who's sending folks to hit us," he elaborated, "we're going to try and not fight with those folks; we're going to hit the bully." This approach, he said, applies in all dimensions including cyber: "If anyone attacks us on cyber, we're going to attack back. We're not going to be feeble," Bennett said.

A screenshot from what is believed to be closed-circuit footage obtained from Iran's Khuzestan Steel Co. factory floor where a piece of heavy machinery on a steel billet production line malfunctions and causes a massive fire, June 27, 2022. (Screenshot: Twitter)

Also speaking at Monday's conference, Israel's National Cyber Directorate chief Gaby Portnoy said Iran had become a "dominant rival" in cyberspace, amid relentless attempts to attack civilian infrastructure in the past year.

"There is no longer only one type of an ideological official enemy. On the one hand, Iran has become our dominant rival in cyber, together with Hezbollah and Hamas," Portnoy said. "We see them, we know how they work, and we are there.

"On the other hand, the spectrum also was stretched to attackers, attack groups, proxies, independent crime organizations, and private people," Portnoy added.

According to data presented by the directorate at the conference, 1,500 cyberattacks on the Israeli home front were foiled over the past year alone.

Brig. Gen. (ret.) Gaby Portnoy, director-general of the Israel National Cyber Directorate. (Avshalom Sassoni/Flash90)

Israel and Iran have for years been involved in a largely clandestine cyberwar that occasionally bubbles to the surface. Israeli officials have accused Iran of attempting to hack Israel's water system in 2020.

In turn, Iran has accused the United States and Israel of cyberattacks that have impaired the country's infrastructure.

Iran disconnected much of its government infrastructure from the internet after the Stuxnet computer virus — widely believed to be a joint US-Israeli creation — disrupted thousands of Iranian centrifuges in the country's nuclear sites in the late 2000s.

In a major incident last year, a cyberattack on Iran's fuel distribution system paralyzed gas stations across the country, leading to long lines of angry motorists. The same anonymous hacking group, Gonjeshke Darande, claimed responsibility for the attack on fuel pumps.

THE TIMES OF ISRAEL

'Mess with Israel, you'll pay a price,' PM warns Iran, after steel plant cyberattack

At Cyber Week event, Bennett says 'wreaking havoc in Tehran' not a policy, but Israel will respond to assaults; 'smart folks' at keyboard can do what commandos do without the risks
EMANUEL FABIAN

Outgoing Prime Minister Naftali Bennett warned Tuesday, a day after Iran's major steel companies were hit by a cyberattack, that anyone who attempts a cyberattack against Israel will "pay a price."

"[The] approach with our enemies, especially Iran... we don't go around wreaking havoc in Tehran — that's never been our policy. Our policy is, if you mess with Israel, you'll pay a price," Bennett said at the Cyber Week conference in Tel Aviv.

He also highlighted the benefits of using cyber warfare over more traditional military offensive methods, noting, "You can get a bunch of smart folks sitting on a keyboard to achieve the same effect... without risking your soldiers' lives."

Monday's large cyberattack forced the state-owned Khuzestan Steel Co. to halt production, and two other major steel producers also reported being targeted.

An anonymous hacking group claimed responsibility on social media for the attack, saying it had targeted Iran's three biggest steel companies in response to the "aggression of the Islamic Republic."

The group, calling itself "Gonjeshke Darande," shared what purported to be closed-circuit footage from the Khuzestan Steel Co. factory floor that showed the malfunction of a piece of heavy machinery on a steel bar production line, causing a massive fire.

Israeli military correspondents, who are regularly briefed off-the-record by senior Israeli officials, hinted that Israel was directly responsible for the assault in retaliation to a suspected cyberattack that caused rocket sirens to be heard in Jerusalem and Eilat last week.

Bennett was asked at the conference about his approach as prime minister to cyber offense and defense, and gave a lengthy, considered response.

Prime Minister Naftali Bennett speaks with Michal Braverman-Blumenstyk, Microsoft corporate VP and CEO of the Israel R&D Center at the annual cybersecurity conference Cyber Week at Tel Aviv University, June 28, 2022. (Cyber Week, Tel Aviv University)

"Today you can get stuff done hitting your enemy through cyber which in the past would require to covertly send 50 or 100 commando soldiers behind enemy lines with huge risk," he said. "And now you can get a bunch of smart folks sitting on a keyboard to achieve the same effect. So it's a no-brainer. And this is why inevitably cyber is going to become one of, if not the most prominent dimensions of future warfare. It just makes sense... If you can get the same effect through cyber without risking your soldiers' lives, obviously it's going to happen."

THE TIMES OF ISRAEL

Gantz says Iran and Hezbollah tried to hack UN peace force, steal deployment data

Speaking at Cyber Week event, defense minister warns Tehran is a leader of cyberterrorism, using 'terrorists with keyboards' as proxies
EMANUEL FABIAN

Defense Minister Benny Gantz on Wednesday said Iran and its Lebanese proxy Hezbollah recently attempted a cyberattack against a United Nations peacekeeping force in southern Lebanon, in order to steal information about its activities in the area.

"The leader of global, conventional terrorism is Iran. This is also true for cyberterrorism," Gantz said at the Cyber Week conference in Tel Aviv. "Iran operates via proxies such as Hezbollah in all dimensions — including cyber.

"Today I can reveal recent malign activities conducted by Iranian security institutions in cooperation with Hezbollah: an attempt to disrupt UNIFIL (United Nations Interim Force in Lebanon) operations," Gantz said.

"They launched a cyber operation with the aim of stealing materials about UNIFIL activities and deployment in the area, for Hezbollah's use," he said. "This is yet another direct attack by Iran and Hezbollah on Lebanese citizens and on Lebanon's stability."

It was not immediately clear if the alleged joint Iranian and Hezbollah cyberattack against the UN peacekeeping force was successful, or when it had occurred.

Responding to Gantz's remarks, UNIFIL said it has "not received any direct information on the alleged incident."

"UNIFIL and the United Nations take cyber-security very seriously and have robust measures in place to protect our data," it added in a statement.

Members of UNIFIL patrol the area of Naqura, south of the Lebanese city of Tyre, on the border with Israel on June 6, 2022. (Mahmoud ZAYYAT / AFP)

Gantz said Israel knows "the cyber systems and operation methods of its opponents," and had identified a trend of Iranian hacker groups operating against Israel, other countries in the Middle East, and the world in recent years.

He said Israel is aware of Iranian terror groups, led by the Islamic Revolutionary Guards Corps, that "have tried to carry out operations against international targets, including charities and government networks in the United States," as well as attempts to influence the US presidential election.

"Following investigations published on this subject, we can confirm that the 'Shahid Kaveh' unit operated by the IRGC, which was revealed about a year ago, conducted research to damage ships, gas stations, and industrial plants in several Western countries including Britain, the US, France and Israel," Gantz said, adding that the foiled attempts were carried out "under the direct instructions of Iran's leadership."

"These new proxies are 'terrorists with keyboards,' yet they are just like any other terrorist. We know who they are, we target them and those who direct them. They are in our sights as we speak — and not just in cyberspace," he said.

"Not a single attack on Israel's citizens will be met with silence. The responsibility for such attacks lies with the countries and terror groups that fund and guide them. There is a variety of possible responses to cyberattacks — in and outside of the cyber domain," Gantz added.

Gantz's comments came two days after a large cyberattack forced the Iranian state-owned Khuzestan Steel Co. to halt production, and two other major steel producers also reported being targeted.

A screenshot from what is believed to be closed-circuit footage obtained from Iran's Khuzestan Steel Co. factory floor where a piece of heavy machinery on a steel billet production line malfunctions and causes a massive fire, June 27, 2022. (Screenshot: Twitter)

Israeli military correspondents, who are regularly briefed off-the-record by senior Israeli officials, hinted that Israel was directly responsible for the assault in retaliation to a suspected cyberattack that caused rocket sirens to be heard in Jerusalem and Eilat last week.

Israel and Iran have for years been involved in a largely clandestine cyberwar that occasionally bubbles to the surface. Israeli officials have accused Iran of attempting to hack Israel's water system in 2020.

During Wednesday's conference, the deputy commander of the military's 8200 intelligence unit said it had foiled that attack. "We thwarted the attempt to take over Israel's critical water systems and poison them several years ago," Col. Aleph, who can be identified only by the initial of his first name, said.

"In another case, we also identified that a certain opponent was attacking Israel, and while we were recognizing that, the same attacker was also trying to target power plants in the US. We were able to prevent this threat through close cooperation with our American partners," he said.

Col. "Aleph", the deputy commander of the IDF's 8200 intelligence unit speaks at the Cyber Week conference in Tel Aviv, June 29, 2022. (Cyber Week, Tel Aviv University)

In turn, Iran has accused the United States and Israel of cyberattacks that have impaired the country's infrastructure.

Iran disconnected much of its government infrastructure from the internet after the Stuxnet computer virus — widely believed to be a joint US-Israeli creation — disrupted thousands of Iranian centrifuges in the country's nuclear sites in the late 2000s.

In a major incident last year, a cyberattack on Iran's fuel distribution system paralyzed gas stations across the country, leading to long lines of angry motorists. The same anonymous hacking group, Gonjeshke Darande, claimed responsibility for the attack on fuel pumps.

In a brief message in Hebrew at the conference, Gantz mentioned a video Hamas released on Tuesday of Hisham al-Sayed, an Israeli man held by the terror group in the Gaza Strip, showing him hooked up to oxygen and claiming his health had deteriorated.

"Yesterday a video was published, and its goal is extortion over a humanitarian issue. Hamas is holding captive for years the four boys against international law, against morals," he said, referring to al-Sayed and Avera Mengistu, and the bodies of two Israeli soldiers, Oron Shaul and Hadar Goldin.

"Hamas is responsible for this, and our expectation is for the international community to act against this behavior. Israel is continuing to act in order to return them home," he said. "It is a humanitarian issue, and blackmail and other tricks will not change our conduct."

THE TIMES OF ISRAEL

Pharma giant Bayer to set up cybersecurity center in Israel

German multinational to operate large local cyber unit tasked with creating partnerships with local tech ecosystem

RICKY BEN-DAVID

Pharmaceutical giant Bayer will open a cybersecurity development center in Israel, as part of the German multinational's global cybersecurity operations, in a bid to engage and partner with one of the strongest Israeli sectors in the local tech ecosystem.

Hugo Hagen, the managing director and country division head of Bayer Israel, made the announcement Wednesday together with the Ministry of Economy and Industry, following the visit to Israel this week of a delegation of senior Bayer executives.

Israel is currently hosting the Cyber Week conference at Tel Aviv University, an annual cybersecurity summit that draws government officials, intelligence authorities, and entrepreneurs and executives from all over the world. Both outgoing Prime Minister Naftali Bennett and Defense Minister Benny Gantz spoke at the conference this year, warning that the cyber sphere was the most prominent dimension of future warfare, including attacks on critical infrastructure such as energy, water and manufacturing, and supply chain operations.

Israel is a cybersecurity powerhouse with companies in the sector raising a record $8.8 billion in 2021, a figure that accounts for 40% of the total funds raised by cybersecurity firms worldwide last year, according to data provided by the Israel National Cyber Directorate.

Overall cybersecurity exports from Israel were estimated at $11 billion in 2021, according to separate Israeli Export Institute data.

A number of multinationals have opened cybersecurity centers in Israel including Mastercard, Japanese IT multinational Fujitsu, Anheuser-Busch InBev (AB InBev), the world's largest beer maker, and multinational consulting firm PricewaterhouseCoopers.

For Bayer, Hagen said in a statement Wednesday: "As a company engaged in R&D in the core areas of life sciences, the ability to integrate with Israel's unique cybersecurity ecosystem, alongside sectors such as medical innovation and agricultural development is an opportunity to integrate as players in the Israeli market and provide added value for Bayer and for the ecosystem."

Biotech and pharmaceutical companies are highly susceptible to cyberattacks, according to experts. In 2017, pharmaceutical giant Merck was one of the high-profile corporate victims of one of the worst, most destructive cyberattacks in the world, NotPetya, a "wiper" malware attributed to Russia. The infection spread across the world from hospitals to shops to banking multinationals, huge corporations, and manufacturers, and cost billions of dollars in losses.

Bayer's cybersecurity center will operate in Bayer Israel's existing offices in the central city of Hod Hasharon, and will work to create collaborations with Israeli cybersecurity startups and companies.

The new center will be one of Bayer's largest internal cyber units, the Ministry of Economy indicated.

The ministry's director-general, Dr. Ron Malka, said Israel was a major draw for multinational companies "and there is no doubt that such connections contribute to employment, innovation, [and] Israel's image and attract other international investments."

Malka welcomed Bayer's expansion in Israel and said the ministry was working to create "similar connections in the future."

Bayer — the inventor of aspirin and the maker of over-the-counter commercial products such as Claritin, Alka-Seltzer and Aleve, as well as prescription cancer medication Nexavar — has been active in Israel since 2008, and has been tapping into local opportunities in both the pharmaceutical field and the agricultural tech sector. The company invested in plant genomics firm Evogene in 2010; in Compugen Ltd., a cancer immunotherapy firm in 2013; and in drip irrigation developer Netafim in 2016.

In 2016, Bayer set up an agricultural innovation fund together with the Trendlines Group, an investment company, to treat bacterial diseases in crops, and has partnered with Israeli biotechnology incubator FutuRx to foster startups focused on innovative therapeutic technologies.

The firm also collaborates with Prospera Technologies to improve agriculture output using the AI and advanced data collecting methods developed by the Israeli startup.

In 2019, a delegation of 15 senior officials of Bayer visited Israel to seek out partnerships and investment opportunities in local startups in the field of biotechnology and digital health. Similar visits had been held until then only in countries considered among the leaders in the field of biotech, pharma and digital innovation, including Germany, China and the United States

The Bayer delegation in Israel, June 29, 2022 with director-general of the Ministry of Economy and Industry Dr. Ron Malka. (Gideon Sharon/ Ministry of Economy and Industry)

Hagen himself has been in Israel since 2019, scouting for Israeli technologies in the fields of pharma, agriculture and digital health technologies for the 150-year-old life sciences German-based firm Bayer AG, one of the largest in the world by sales.

In an interview with The Times of Israel last year, Hagen said his job was to "ping" managers at the HQ about what is going on in the local ecosystem, alerting them about the latest developments. Competition to find the next big thing in Israel is high.

"There are so many companies scouting for those good ideas," he said. "If there is an Israeli company with good phase II (clinical trial) data, I'll promise you it is on the radar already of many pharma companies."

Cyber Week
June 27th-30th, 2022
Tel Aviv University, Israel

Yuval Ne'eman Workshop for Science, Technology and Security Tel Aviv University
ICRC Blavatnik Interdisciplinary Cyber Research Center
TEL AVIV UNIVERSITY אוניברסיטת תל אביב
Cyber Israel National Cyber Directorate
In cooperation with:
Ministry of Foreign Affairs Israel
ISRAEL CYBER ALLIANCE
State of Israel Ministry of Economy and Industry Foreign Trade Administration
ISRAEL EXPORT INSTITUTE

Last year, Bayer's investment arm, Leaps, invested in Israel-founded biotech firm Ukko, which raised a total of $40 million from investors in a series B funding round to use artificial intelligence and protein engineering to develop healthier food and therapies for food allergies.

Bayer also signed a collaboration agreement last June to test out new drugs on human heart tissue 3D-printed by researchers at Tel Aviv University.

But the German multinational has yet to make any acquisitions of Israeli firms and has faced a period of unprecedented turbulence following its 2016 purchase of US agritech firm Monsanto for $66 billion. Along with the company, Bayer acquired what turned out to be over $10 billion in lawsuit settlements stemming from the use of Monsanto's weed-killer Roundup, which allegedly causes cancer. Its market capitalization dropped from a high of $116.8 billion in 2017 to just $46.1 billion in late 2020. It has since recovered to about $63 billion as of June 2022.

Hugo Hagen, the managing director and country division head of Bayer Israel (Danit Nitzan)

THE JERUSALEM POST

'Only Israel teaches cybersecurity in high schools'

Isaac Ben-Israel, the man who kick-started country's cyber revolution, gives insight on defense technology, recent examples of tech warfare

• By ZACHY HENNESSY

The annual international cybersecurity CyberWeek event is kicking off on Monday in Tel Aviv.

Cybersecurity experts, industry leaders, start-ups, investors, academics, diplomats and government officials will gather for a thought-provoking exchange of knowledge, methods and ideas related to the cybersecurity industry and the fields surrounding it.

More than 40 round tables, panels, workshops, forums, BSides and competitions will take place at the weeklong event.

Prof. Isaac Ben-Israel, director of the Blavatnik Interdisciplinary Cyber Research Center at Tel Aviv University, is a co-founder of the annual event. A major-general in the IDF, he served in several top defense technology units until his retirement in 2002.

In 2011, he submitted the National Cyber Initiative to the government, a plan that laid the foundation for Israel's cyber revolution during the past decade.

In an interview with *The Jerusalem Post*, Ben-Israel elaborated on CyberWeek's foundation and the lessons to be learned from recent examples of cyber warfare.

How would you define the fundamental idea of CyberWeek? Is there really enough to go over to take up a whole week?

From the beginning, the main idea was – and still is – to regard cyber activity as a kind of interdisciplinary discipline. It's not only about technology.

Although most of the problems in the 21st century we tend to solve with technology, many times those problems are not purely technological.

Solving these problems, many times, may depend on variables, like the psychology of the user, or sometimes the psychology of the masses, when looking at things like social media.

One often has to take into account legal problems, [or] the conflict between different sets of values, like security on the one hand and privacy on the other hand.

We could also make cybersecurity much more efficient if we disregard the privacy or human rights of our own citizens – which is, in a way, a philosophical question. These factors have nothing to do with technology.

Next week, you will find people from many disciplines: computer scientists, engineers, etc, but there are also people that are involved in policy and legal issues, psychology, you name it: all the issues that I mentioned.

That is the nature of CyberWeek, from day one until today. That's why we need a week. We started with a one-day conference and then we said, 'Okay, but we have to discuss the legal issues, we have to discuss ransomware, we have to discuss human psychology, business issues.' We had to keep extending it.

Do you see CyberWeek as the big Israeli cybersecurity conference or as the big cybersecurity conference that happens to be in Israel?

There is not much difference between the two, because while we didn't invent the technology in Israel, we were among a very small group of countries which used it for intelligence and defense.

What we were the first to do, in a way, was to come out of the closet with our cybersecurity knowledge. In 2011, we decided not to keep it a secret anymore. We made it a legitimate subject for normal civilian activity. We started to develop academic centers.

It's hard to believe but when we started in 2011, there was not even one university on the globe in which you could go and study cybersecurity. Why?

Because if you publish a paper about it in a university, the enemy will also read it. So the attitude was to keep it secret.

Today, we are the only country in the world where we teach cybersecurity in high schools. But that gives us an advantage. When people all around the world would like to go and see what is in the fault line or cybersecurity, they will usually find it in Israel.

Moving away from CyberWeek, I wanted to pick your brain on the cyberwarfare that was reported at the onset of the Russia-Ukraine conflict.

Why haven't we heard about more cyberattacks between the two countries as the war has waged on?

Usually, when you build a certain offensive capability – tanks, aircraft, submarines – you can assume that 20 years from now the situation will be different, and everything you prepared 20 years before may not fit the new battle arena.

So part of military organization is to track the changes on the other side, and if you come to the conclusion that the weapons that you already have do not fit the situation anymore, you modify your weapons or develop a new generation of weapons.

It's an endless game: you prepare certain capabilities, you follow the changes on the other side, you modify your capabilities.

The same also holds for cyber weapons. The only difference is that the timescale is very short. You cannot expect tools that you developed six years ago to operate today, because the probability that the victims will [still] have the same architecture is almost zero.

In the cyber field, six years is like five generations.

If you want your capability to be adaptive, you have to invest a huge effort in maintaining this capability. Russia didn't do that, and that's why when the war started, you saw certain cyber actions, but that was the end of it.

Does the same idea apply to the back-and-forth of cyberattacks between Israel and Iran?

It's not the same because, outside of a wartime scenario, both sides have a lot of time to develop their attacks. Our exchange of attacks aren't really things that are improvised on the spot. If you need another month, you can take another month to develop. It's different.

Still, it demonstrates other things. Until now, all the Iranian attempts to cause damage to Israel via cyber technology have been very marginal.

This may change at any time, but until now, they've tried but failed. That shows us that the tools we built for protecting ourselves are effective, but that doesn't mean that we can sleep on the job – because they're definitely trying.

MAJ.-GEN. (ret.) Prof. Isaac Ben-Israel. (Yuval Ne'eman Workshop for Science Technology and Security)

Come and discover Beresheet – a new residential experience for people ages 65 and over, which is being built at Ramat Motza in the Jerusalem mountains. Here you have the opportunity to be the pioneers and partners in a new residential concept and to take part in building a way of life that fits your worldview. Come and build a life full of meaning and interest together with people who know how to appreciate the amazing nature and landscape that surrounds the project, enjoy the atmosphere of Shabbat Kodesh and celebrate the Israeli holidays with a strong and cohesive community, which we built together.

*2349

Beresheet Senior Living Community – Jerusalem Hills –

Last Chance for Pre-Sale Prices Occupancy August 2023

Cyber Week
June 27th-30th, 2022
Tel Aviv University, Israel
Yuval Ne'eman Workshop for Science, Technology and Security Tel Aviv University
ICRC Blavatnik Interdisciplinary Cyber Research Center
TEL AVIV UNIVERSITY אוניברסיטת תל אביב
Cyber Israel National Cyber Directorate
In cooperation with:
Ministry of Foreign Affairs Israel
ISRAEL CYBER ALLIANCE
State of Israel Ministry of Economy and Industry Foreign Trade Administration
ISRAEL EXPORT INSTITUTE

THE JERUSALEM POST

BENNETT CYBER WARNING TO IRAN:

If you mess with us, you'll pay a price

• By YONAH JEREMY BOB

Prime Minister Naftali Bennett warned Iran that in the cyber arena, if you mess with Israel, you will pay a price.

"Just like there is nuclear deterrence, there is going to be cyber deterrence," he said on Tuesday at the Tel Aviv University Cyber Week. "My approach generally, and especially with Iran, is – and we don't go around wreaking havoc in Tehran, that has never been our policy – but our policy is if you mess with Israel, you'll pay a price. You can no longer hit Israel indirectly and through proxies and think you'll get away with it.

NEW NATIONAL cybersecurity chief Gaby Portnoy addresses the Tel Aviv University conference yesterday. (Cyber Week, Tel Aviv University)

"If you are a bully who sends folks, we will try to hit you" with kinetic, covert and cyber. "Anyone attacking us in cyber, we are going to attack back. We are not going to be feeble here. We can get stuff done hitting your enemy through cyber. Before we needed to send 50 to 100 commandos behind enemy lines with huge risks. Now we get a bunch of smart folks together sitting at a keyboard and achieve the same effect. It is inevitable that cyber is going to become one, if not the most, prominent dimension of future warfare."

Regarding defending the private sector from cyberattacks, Bennett said that "Israel has a layered approach. I appointed a new [Israel National Cyber Directorate] chief, [Gaby] Portnoy. Corporations must take their own responsibility, the law does apply that when they screw up with their clients, that is their problem. So they have an incentive to take care of themselves."

Bennett added, "That is not enough. The national-level

See PRICE, Page 7

THE JERUSALEM POST

Iran trying to disrupt UN Lebanon peace force with cyberattacks – Gantz

• By ANNA AHRONHEIM

Iran is trying to disrupt UNIFIL in Lebanon in cooperation with Hezbollah by "carrying out a cyber operation aimed at stealing materials about UNIFIL's deployment in the area for the use of Hezbollah," Defense Minister Benny Gantz said Tuesday at the International Cyber Conference.

"This is another attack by Iran and Hezbollah on Lebanese citizens, and on Lebanon's stability," he said.

According to Gantz, Iran is challenging Israel not only in the air, land and at sea, but has been waging cyberattacks against it for over a decade. While Israel faced several significant cyberattacks a decade ago, it now faces over 1,000 attacks a year.

"Governments and democracies are tasked with defense and deterrence," he said. "We must charge a heavy price from those who attempt to harm us and this is how Israel operates. The cyber dimension is boundless but not without traces. It's important to emphasize that Israel

See FORCE, Page 7

The link between IRGC and Venezuelan plane

• By TZVI JOFFRE

The recent detainment of a Venezuelan cargo plane in Argentina could be linked to attempts by the Islamic Revolutionary Guards Corps (IRGC) to attack Israelis abroad, according to independent Israeli intelligence analyst Ronen Solomon, who runs the Intelli Times blog.

The cargo plane, which belongs to the Venezuelan state-owned Emtrasur cargo company, was detained on June 8 after landing in Buenos Aires. There were concerns

See PLANE, Page 7

THE JERUSALEM POST

Was Iran behind siren cyberattacks in Jerusalem, Eilat?

A diplomatic source said the hacker identity is uncertain, but suspicions have been raised that the cyberattack was carried out by Iran.

YONAH JEREMY BOB

False rocket warning sirens that were activated in Jerusalem and Eilat on Sunday evening were likely caused by a cyberattack, the Israel National Cyber Directorate (INCD) confirmed on Monday morning.

By Monday, there was rampant speculation that Iran was the perpetrator of the hack, with a slew of cyber experts opining as such in interviews about the possibility of Iranian involvement.

However, a diplomatic source said there was still uncertainty whether the Islamic Republic was the source of the attack.

The diplomatic source also downplayed the significance of the attack, saying, "There is constant cyber activity against Israel. In terms of Israel working on increasing its cyber resilience, it is not in a bad place. Part of the [state's] multi-year plan is to build a cyber iron dome in cooperation with other nations. The headlines exaggerated about the sirens yesterday."

On Sunday evening, rocket sirens sounded for almost an hour in Eilat and across several Jerusalem neighborhoods including Talpiot, Katamon and Beit Hakerem.

Was it really a cyberattack?

The IDF initially said there was a system malfunction by the IDF, although the actual cause was unknown.

The INCD said the attack was directed against the municipal siren systems rather than through the IDF Home Front Command alert system, which is usually viewed as more secure.

The relevant authorities were instructed to take preventative measures against the threat.

Speaking to Army Radio on Monday morning, former IDF deputy chief of staff MK Yair Golan (Meretz) responded to the report, saying that Israel was preparing itself for Iranian attempts to harm the country through cyberwarfare.

"The Home Front Command's alarm system was not breached, the municipal siren system was, but it is very worrying and disturbing," Golan said. "If there is a breach point there, it should be closed immediately."

The idea that someone else besides Iran would be behind the hack is hard to explain. There was no ransomware or monetary extortion element to the attack, which mostly disqualifies criminals.

Few nation states with powerful cyber programs besides Iran are in conflict with Israel. Even if, for example, Russia decided to retaliate against Jerusalem for its support for Ukraine, playing with sirens would seem to be beneath it.

In contrast, infiltrating a non-essential and less protected system that could get significant media attention, like the sirens, would fit into prior Iranian cyberattacks.

Cyberattacks on Iran

Last week, Iran claimed that it had uncovered a cyberattack on the municipality of Tehran. The attack impacted traffic cameras and other electronic services, but an Iranian official said it did not compromise any critical data.

Most cyberattacks on Iran have been laid at Israel's doorstep, though there are some Iranian dissidents and human rights activists who have also hacked the Islamic Republic.

If Iran was behind Sunday night's cyberattack, it would be another move in a long and cyclical cyberwarfare game between the countries that has escalated since spring 2020.

Omree Wechsler, a senior researcher at the Blavatnik Interdisciplinary Cyber Research Center, commented on "the story of Iranian cyberattack that may be behind false rocket warning sirens in Jerusalem. Specifically, the hacks targeted public address systems in Jerusalem and Eilat. As a clear Israeli symbol, it shows that this is an opportunistic attack and not a sophisticated and well-planned attack launched years ago. The hackers attacked where they found loopholes."

"The hackers attacked where they found loopholes."

Omree Wechsler, senior researcher, Blavatnik Interdisciplinary Cyber Research Center

Wechsler added, "As many cyberattacks in the world are focused on financial or espionage targets, the Iranian activity against Israel is in accordance with the pattern of causing damage or creating panic. Such attacks are common and are part of a daily routine that includes thousands of attempts to hack into any system or server whose damage would cause media coverage."

THE JERUSALEM POST

Iran trying to disrupt UNIFIL in Lebanon with cyberattacks - Gantz

Iran trying to disrupt UNIFIL in Lebanon with cyberattacks - Gantz "Israel knows the cyber systems and operational methods of its opponent."
ANNA AHRONHEIM

Iran is trying to disrupt UNIFIL in Lebanon in cooperation with Hezbollah by "carrying out a cyber operation aimed at stealing materials about UNIFIL's deployment in the area for the use of Hezbollah," Defense Minister Benny Gantz said Tuesday at the International Cyber Conference.

"This is another attack by Iran and Hezbollah on Lebanese citizens, and on Lebanon's stability," he said.

According to Gantz, Iran is challenging Israel not only in the air, land and at sea, but has been waging cyberattacks against it for over a decade. While Israel faced several significant cyberattacks a decade ago, it now faces over 1,000 attacks a year.

"Governments and democracies are tasked with defense and deterrence. We must charge a heavy price from those who attempt to harm us and this is how Israel operates. The cyber dimension is boundless but not without traces."

"Governments and democracies are tasked with defense and deterrence," he said. "We must charge a heavy price from those who attempt to harm us and this is how Israel operates. The cyber dimension is boundless but not without traces. It's important to emphasize that Israel knows the cyber systems and operational methods of its opponent."

Iran is not only the "leader of global conventional terrorism," Gantz noted, it is also using hacker groups to conduct attacks against Israel and other countries in the region and the world

Iran's hack attacks

Iran, "threatens to damage global infrastructure, it aims to spread fear, and it even attempts to influence democratic processes and governments," he said. It attempted to influence the US presidential election. It also tried to carry out cyber operations against international targets like charities and government networks in the US.

Gantz confirmed that the Shahid Kaveh unit operated by Iran's Islamic Revolutionary Guard Corps conducted research to damage ships, gas stations and industrial plants in several Western countries including Britain, the United States, France and Israel.

Last year, classified documents, allegedly from Iran, revealed secret research conducted by the unit into how a cyberattack could be used to sink a cargo ship or blow up a fuel pump at a gas station.

The internal files, about 57 pages of five research reports, were obtained by Sky News, which quoted an unnamed source as saying that he believed the work was "evidence of efforts by Iran to collect intelligence on civilian infrastructure that could be used to identify targets for future cyberattacks."

In order to thwart such attacks, Israel "works closely with our partners. The same cooperation frameworks that we are building in the region vis-à-vis Iran are also expanding to the cyber dimension," Gantz said. "Together we can prevent significant harm to the citizens of the region and the world."

The defense minister said that the responsibility for these sorts of attacks lies with the governments and terrorist groups that guide the proxies which he called "terrorists with keyboards." He warned that there are a "variety" of possible responses to cyberattacks, in and outside the cyber domain.

"They are just like any other terrorist," Gantz said. "We know who they are, we target them and those who direct them. They are in our sights as we speak – and not just in cyberspace. Not a single attack on Israel's citizens will go by silently."

THE JERUSALEM POST

IDF stopped hackers from hitting US power plants - Unit 8200 official

This is the first time a current Unit 8200 official, deputy chief of IDF Unit 8200, "Col. U.," discussed such sensitive cyber intelligence sharing in public.

YONAH JEREMY BOB

IDF Unit 8200 deputy chief Col. U. is seen speaking at Tel Aviv University's annual Cyber Week, on June 29, 2022.

The deputy chief of IDF Unit 8200, "Col. U.," on Wednesday said that his intelligence agency warned the United States of attempts to hack the country's power plants in time to thwart the cyberattack.

Col. U. speaks up

Although this was not the first time these warnings to the US have been made public, it was the first time a Unit 8200 official had discussed sensitive cyber intelligence in public.

The most well-known example was Israel's 2017 warning to the US about Russia's Kaspersky antivirus software being used as a way to backdoor spy on them or plant malware.

Col. U. recalled that an "adversary [Iran] attacked water facilities in Israel. We saw this attacker attempting to poison the water in an attempt to claim human lives. We mitigated that threat far ahead.

"Another adversary attacked Israel [and in the process of stopping the cyberattack,] we also found that they were attempting to target US power plants as well," he said. "This was the first indication of this attack. It enabled preventing this threat through tight collaboration with our fantastic American partners."

In 2020, then-energy minister Yuval Steinitz revealed an attempted cyberattack on Israel's energy sector, which was thwarted.

"We're Israel's SIGINT"

Introducing his unit, U. said, "We're Israel's national SIGINT [Signal Intelligence] and Cyber Unit and are part of the defense intelligence in the IDF. Our mission is intelligence collection and [combating] crucial threats to Israel for the IDF and for Israel's policymakers. We are also a major player in the cyber domain in Israel and in Israel's cyberdefense."

"We're Israel's national SIGINT [Signal Intelligence] and Cyber Unit and are part of the defense intelligence in the IDF. Our mission is intelligence collection and [combating] crucial threats to Israel for the IDF and for Israel's policymakers."

Col. U.

"Like it or not, we work in quite a tough neighborhood. This leads to ongoing high friction in a dynamic and intense environment," said U. "We have new challenges each day. When we succeed we save lives. When we fail this becomes a major problem for our nation."

"Counter cyber operations are a major part of our operations," he added. "Once we obtain superiority over the attacker, we then act to deny their capabilities. First of all, by collaborating with industry and other agencies, but, if necessary, we do it on our own, implementing 'our tools' at some point, somewhere along the attack stream. 8200 won't rest until the threat is removed.

"We are privileged to have a huge amount of talent. Each year, we recruit between 1,000 to 2,000 of the brightest girls and boys in Israel as they join the IDF at the age of 18. This also makes our personnel very young. 73% are under the age of 23."

"Our core values are democratic values and ethics. We have military decision-making procedures while allowing individuals to express their opinions and concerns," the Unit 8200 deputy chief said.

"We are here and we are willing to collaborate. Most of what we do will have to remain top secret, but some aspects of the way we do it can and should be discussed. We are preventing cyber threats against Israelis and we ensure that Israel remains the leading power in technology and cyber in our region."

THE JERUSALEM POST

Israel cyber chief: Iran has become our dominant rival in cyber

Israel National Cyber Directorate (INCD) Chief Gaby Portnoy: "We see them, we know how they work and we are there."
YONAH JEREMY BOB

Iran has become our dominant rival in cyber together with Hezbollah and Hamas, Israel National Cyber Directorate (INCD) Chief Gaby Portnoy said on Tuesday.

Speaking at Tel Aviv University's Cyber Week, he said, "We see them, we know how they work and we are there."

"We see them, we know how they work and we are there."

INCD Chief Gaby Portnoy

Portnoy made his comments a day after Iran's steel industry took one of its biggest cyber hits in history, bringing it to a grinding halt and only days after an Iranian cyberattack on Israel's siren early warning systems in Jerusalem and Eilat.

'Experience of Resurrection': Jerusalem hi-tech religious experiences

The INCD chief said Israel is building a "cyber iron dome" which will elevate cybersecurity by using new mechanisms with cyber parameters that will "reduce cyberattacks, provide new big data and an AI overall approach to synchronize nationwide real-time detection... for ongoing cyberdefense efforts."

He said, "we are moving faster from resilience to proactive defense," trying to come after cyber attackers in their digital safe havens where they had planned attacks in the past without interference.

Further, he said we "need cybersecurity protocols for infrastructure" to be used also for the wider public, including extending tools and skills to the entire private sector and down supply chains.

Even smaller businesses need help to understand cyber threat intelligence and with capacity building for their defense to contribute to the national cyberdefense.

THE JERUSALEM POST

Bennett cyber warning to Iran: 'If you mess with Israel, you'll pay a price'

Bennett described the future of Israel's cyber warfare capabilities as replacing dozens of commandos with keyboards.
YONAH JEREMY BOB

Prime Minister Naftali Bennett at Cyber Week

Iran will "pay a price" if it interferes with Israeli cyber-infrastructure, Prime Minister Naftali Bennett warned on Tuesday.

Speaking at the Tel Aviv University Cyber Week, Bennett said, "just like there is nuclear deterrence, there is going to be cyber deterrence. My approach generally, and especially with Iran is – and we don't go around wreaking havoc in Tehran, that has never been our policy - but our policy is if you mess with Israel you'll pay a price."

"You can no longer hit Israel indirectly and through proxies and think you'll get away with it."

Future cyber warfare

"You can no longer hit Israel indirectly and through proxies and think you'll get away with it," Bennett continued.

The prime minister said, "if you are a bully who sends folks - we will try to hit you," with kinetic, covert and cyber, adding "anyone attacking us in cyber, we are going to attack back. We are not going to be feeble here."

Bennett stated, "we can get stuff done hitting your enemy through cyber. Before we needed to send 50-100 commandos behind enemy lines with huge risks."

"Now we get a bunch of smart folks together sitting at a keyboard and achieve the same effect...It is inevitable that cyber is going to become one, if not the most, prominent dimension of future warfare," he said.

THE JERUSALEM POST

Founder of the upcoming CyberWeek weighs in on Russia and Iran's cyber warfare attempts

Isaac Ben-Israel, the man who kickstarted the Israel's cyber revolution, gives insight into cybersecurity's many facets.

ZACHY HENNESSEY

The annual international cybersecurity CyberWeek event is kicking off on Monday in Tel Aviv. Cybersecurity experts, industry leaders, start-ups, investors, academics, diplomats and government officials will gather for a thought-provoking exchange of knowledge, methods and ideas related to the cybersecurity industry and the fields surrounding it. More than 40 round tables, panels, workshops, forums, BSides and competitions will take place at the weeklong event.

Prof. Isaac Ben-Israel, director of the Blavatnik Interdisciplinary Cyber Research Center at Tel Aviv University, is a co-founder of the annual event. A major-general in the IDF, he served in several top defense technology units until his retirement in 2002. In 2011, he submitted the National Cyber Initiative to the government, a plan that laid the foundation for Israel's cyber revolution during the past decade.

How would you define the fundamental idea of CyberWeek? Is there really enough to go over to take up a whole week?

From the beginning, the main idea was – and still is – to regard cyber activity as a kind of interdisciplinary discipline. It's not only about technology. Although most of the problems in the 21st century we tend to solve with technology, many times those problems are not purely technological. Solving these problems, many times, may depend on variables, like the psychology of the user, or sometimes the psychology of the masses, when looking at things like social media.

One often has to take into account legal problems, [or] the conflict between different sets of values, like security on the one hand and privacy on the other hand. We could also make cybersecurity much more efficient if we disregard the privacy or human rights of our own citizens – which is, in a way, a philosophical question. These factors have nothing to do with technology.

We started with a one-day conference and then we said, 'Okay, but we have to discuss the legal issues, we have to discuss ransomware, we have to discuss human psychology, business issues.' We had to keep extending it."

Prof. Isaac Ben-Israel, Director, Blavatnik Interdisciplinary Cyber Research Center, Tel Aviv University

Next week, you will find people from many disciplines: computer scientists, engineers, etc, but there are also people that are involved in policy and legal issues, psychology, you name it: all the issues that I mentioned. That is the nature of CyberWeek, from day one until today. That's why we need a week. We started with a one-day conference and then we said, 'Okay, but we have to discuss the legal issues, we have to discuss ransomware, we have to discuss human psychology, business issues.' We had to keep extending it.

Do you see CyberWeek as the big Israeli cybersecurity conference or as the big cybersecurity conference that happens to be in Israel?

Do you see CyberWeek as the big Israeli cybersecurity conference or as the big cybersecurity conference that happens to be in Israel?

There is not much difference between the two, because while we didn't invent the technology in Israel, we were among a very small group of countries which used it for intelligence and defense.

What we were the first to do, in a way, was to come out of the closet with our cybersecurity knowledge. In 2011, we decided not to keep it a secret anymore. We made it a legitimate subject for normal civilian activity. We started to develop academic centers.

It's hard to believe but when we started in 2011, there was not even one university on the globe in which you could go and study cybersecurity. Why? Because if you publish a paper about it in a university, the enemy will also read it. So the attitude was to keep it secret.

Today, we are the only country in the world where we teach cybersecurity in high schools. But that gives us an advantage. When people all around the world would like to go and see what is in the fault line or cybersecurity, they will usually find it in Israel.

Moving away from CyberWeek, I wanted to pick your brain on the cyberwarfare that was reported at the onset of the Russia-Ukraine conflict. Why haven't we heard about more cyberattacks between the two countries as the war has waged on?

Usually, when you build a certain offensive capability – tanks, aircraft, submarines – you can assume that 20 years from now the situation will be different, and everything you prepared 20 years before may not fit the new battle arena. So part of military organization is to track the changes on the other side, and if you come to the conclusion that the weapons that you already have do not fit the situation anymore, you modify your weapons or develop a new generation of weapons. It's an endless game: you prepare certain capabilities, you follow the changes on the other side, you modify your capabilities.

The same also holds for cyber weapons. The only difference is that the timescale is very short. You cannot expect tools that you developed six years ago to operate today, because the probability that the victims will [still] have the same architecture is almost zero. In the cyber field, six years is like five generations.

If you want your capability to be adaptive, you have to invest a huge effort in maintaining this capability. Russia didn't do that, and that's why when the war started, you saw certain cyber actions, but that was the end of it.

Does the same idea apply to the back-and-forth of cyberattacks between Israel and Iran?

It's not the same because, outside of a wartime scenario, both sides have a lot of time to develop their attacks. Our exchange of attacks aren't really things that are improvised on the spot. If you need another month, you can take another month to develop. It's different.

Still, it demonstrates other things. Until now, all the Iranian attempts to cause damage to Israel via cyber technology have been very marginal. This may change at any time, but until now, they've tried but failed. That shows us that the tools we built for protecting ourselves are effective, but that doesn't mean that we can sleep on the job – because they're definitely trying.

THE JERUSALEM POST

World War III will be a cyber war but the world isn't ready - comptroller

Israel's State Comptroller Matanyahu Englman explains the deficiencies of Israel's public cybersecurity

ZACHY HENNESSEY

Israel's State Comptroller Matanyahu Englman

"World War III will be a cyberwar, but the world is not prepared for cyberattacks," said Israel's State Comptroller Matanyahu Englman on Wednesday.

During a panel at Cyber Week 2022, Englman gave a grim statement on the current state of public cyber security. "In a way, we all are living inside the global 'Big Brother' show," he warned. "We are exposed. The citizens of the world have no protection. Our data are visible to too many people. Our money is exposed; our children are exposed; our health is exposed; our security is exposed."

"We are exposed. The citizens of the world have no protection. Our data are visible to too many people. Our money is exposed; our children are exposed; our health is exposed; our security is exposed."

He explained that the vulnerabilities that the Israeli public faces in the cyber arena have inspired his decision to focus on cybersecurity in his official duties, noting that "in view of the growing cyber threats faced by the State of Israel in recent years, I have decided to place the cyber field as one of the core issues the [state] audit will address."

As such, Englman established a cyber audit division, as well as a dedicated division for information systems auditing within the State Comptroller's Office. "At first, there were those who raised an eyebrow; today there is no one who does not understand the importance of the subject," he said.

He elaborated on the details of the cyber audit process, stating that it will examine privacy protection, control and protection mechanisms of computerized systems, investment in IT and cybersecurity, advance preparedness for cyber incidents and disaster recovery, a raised level of logical and physical protection, insurance coverage and more.

These topics are to be examined from several perspectives: cyberattacks and damage to critical state infrastructure; public expenditure in the field of IT and the rate of expenditure on cyber protection; and privacy infringement.

"For example, we examined the protection of biometric databases," Englman said. "We found that the Transportation Ministry does not examine aspects of information security and protection of passenger privacy of the 'Rav Kav' – a database operated by public transportation companies that include photos of about a million children and information about their travels."

On that note, in February 2022, Englman's office published a special report on the protection of children and youth in the online space.

Prior cyber audits have uncovered several key insights, said Englman. "It was found that the law enforcement authorities in Israel do not have the ability to contend with cybercrime and ransomware. Eighty-seven percent of cybercrime victims in Israel in 2019 (about two hundred thousand people) did not report the crimes to the police."

He also noted, "A report on the computer system of the Central Election Commission in Israel found that their main computer system began operating in 2008 and it [became 13 years old] last year – and yet, cyber audits were conducted only during election periods, so it was not possible to conduct comprehensive and complex tests that included all aspects required under cyberdefense theory."

"The National Cyber Directorate is empowered to guide several entities that hold critical national infrastructures," he said. "However, the audit found that entire sectors do not have a guide in the cyber field, including the health sector, the transport sector, local government and more."

Englman listed several deficiencies discovered during the audit of critical Israeli infrastructures such as the Traffic Management Center in Jerusalem, hospitals and the Tax Authority systems.

"In the audits, we found significant deficiencies, including that very few penetration tests were performed by public bodies and some of them conducted penetration tests only during the audit, [as well as] the absence of a test environment for performing these tests, and other deficiencies that arose in the penetration tests we conducted, some of which were rectified in the course of the audit," he said.

"The auditing world views cyber risks as a major risk," concluded Englman. "The challenges involved in coping with the matter are complex and they require continuous cooperation between states, for optimal contention with cyber risks. We in the State Comptroller's Office are committed to continuing to address this significant topic even more forcefully, for the benefit of the citizens of Israel and the entire world."

THE JERUSALEM POST

Israeli global cybersecurity summit kicks off with int'l leaders

The five-day conference will also focus on the economic and geopolitical impact on cybersecurity across various domains.

Israel's premier global cybersecurity summit, the global CISO Summit led by Team8, kicked off on Wednesday, with more than 100 Chief Information Security Officers (CISOs) from some of the world's leading companies present.

From Unilever to Walmart, some of the biggest brands in the world had representation in attendance to meet with Israeli cybersecurity professionals and start-ups, where they discuss the future of cybersecurity, as well as the shifting approaches to keep attackers at bay.

The five-day conference will also focus on the economic and geopolitical impact on cybersecurity across various domains, with an emphasis on the increasing importance of the CISO role and its influence on organizations' business strategies.

"In recent weeks we have witnessed significant changes, characterized by de-globalization and economic slowdown, which are dramatically affecting the world, and may also directly impact the frequency of cyberattacks, making the cyber arena more significant than ever."

"In recent weeks we have witnessed significant changes, characterized by de-globalization and economic slowdown, which are dramatically affecting the world, and may also directly impact the frequency of cyberattacks, making the cyber arena more significant than ever," said Team8 Managing Partner Nadav Zafrir.

"At Team8 we have identified a real need to bring together the best cyber experts in the world, including 100 CISOs from well-known companies, and thought leaders from the Israeli cyber industry for five full days of in-depth discussions. Together, we will be better equipped to understand the challenges and opportunities we face, and better positioned to plan accordingly."

The summit

The closing event of the CISO summit, sponsored by Deloitte, Leumi-Tech, Meitar Law Office, Valley Bank, Palo Alto, FinSec - Mastercard, and Enel's Innovation Lab, will coincide with the official opening event of Tel Aviv University's Israeli Cyber Week which takes place from June 27-30. This event will be co-hosted by Team8 alongside these sponsors.

Featured speakers at the event include Renee Wynn, Former NASA Chief Information Officer, Admiral Mike Rogers, former director of the NSA and Operating Partner at Team8, Nadav Zafrir, former 8200 unit commander and Managing Partner at Team8.

The Team8 CISO Village is comprised of hundreds of C-level executives from the world's leading enterprises. Its primary focus is to facilitate collaboration among the world's leading companies with the goal of generating business opportunities for all parties.

By helping Team8 to identify real pain points and understand the requirements of large organizations, members of the Village are first in line to leverage solutions that are purpose-built by Team8 portfolio companies to accommodate their needs.

Some Israeli start-ups in attendance include: Claroty, Sygnia, Talon, Akeyless, Illusive, Cyberpion, Silverfort, Authomize, Cardinal, Orca Security, Ermetic, Safebreach, and Resilion.

THE JERUSALEM POST

Brutal Russian invasion of Ukraine has transformed cybersecurity - UK cyber chief

British National Cyber Security Center CEO Linda Cameron said that the lives of millions of innocent people are in jeopardy due to cyber threats, just like on the battlefield.

YONAH JEREMY BOB

"The brutal Russian invasion of Ukraine has transformed the context of cybersecurity" worldwide, said British National Cyber Security Center CEO Linda Cameron.

Speaking at the Tel Aviv University Cyber Week on Tuesday, Cameron said that the lives of millions of innocent people are in jeopardy due to cyber threats, just like on the battlefield, but that "Ukrainian cyber defenders repelled the attacks and are real heroes."

Even as the world is focused on the Russian threat to Ukraine and Eastern Europe, the UK cyber chief said, "We must not lose sight of the longer-term strategic challenges from China as a technological and economic power," since Beijing is spreading across the globe with "cyber and technology for control."

When tech is used by the wrong hands

She warned of using technologies developed by authoritarian countries that could be used to passively and quietly influence and limit the choices of people in free countries.

"The democracies of the world have to develop technology and systems that avoid products that are not in line with our values," said Cameron.

Moreover, she added, "I hope the Start-Up Nation of Israel can play an important role" in providing the free world with such technologies. "Ransomware attacks strike hard and fast, evolve rapidly, and are all-pervasive, lowering the bar for entry into cybercrime."

When the attacks don't stop

While democracies are starting to better handle mega cyber attacks, she said, they are still behind in fending off hundreds of medium and smaller attacks picking off small and medium businesses that can also impact the country's stability.

Cameron said the key to combating ransomware was to drive down the profit to make it "an unprofitable and unattractive business" for cyber criminals.

Cameron highlighted her agency's successful removal of 3.1 million malicious URLs in 2021, handling more than six billion requests for protection from DNS issues, and shutting down 76,000 online scams based on referrals of suspicious emails from the British general public.

Top US official on cybersecurity Anne Neuberger agreed that Russia's attack on Ukraine profoundly affected the international system, including in cyberspace.

The deputy national security adviser and former top NSA cyber official highlighted various executive orders by the Biden administration that have shifted the burden of responsibility for hacks to corporations that could prevent the hacks, whether they are a direct service provider or a software supplier.

Neuberger listed four key areas to improve in:

Securing critical infrastructure to protect national decision-making and making software more secure;

Working with partners to prepare for cyber incidents before they happen, including expanding cyber resources aid to allies as was done in Ukraine;

Reinforcing norms of enforceable cyber, including at the UN and a 36-nation counter-ransom ware initiative;

Implementing the Department of Defense's "defend forward" approach of holding state and non-state actors responsible for attacks, just like in the physical world.

US National Cyber Director Chris Inglis said everyone must realize that the cyber sphere should be subordinate and does not exist for its own sake.

Recalling the Colonial Pipeline mega hack that shook the US petroleum industry, Inglis said what was so disconcerting was that it was caused by "one single individual, whose private network was not properly configured."

Recalling the Colonial Pipeline mega hack in May 2021 that shook the US petroleum industry, Inglis said what was so disconcerting was that it was caused by "one single individual, whose private network was not properly configured."

He said the hackers "found if they beat one person, they could beat us all. This is a terrible situation. We need to make it so that to beat any one of us, they need to beat all of us. We need to not just get the technology right, we need to get the doctrine right. We need to get people in the right place and then we can bend technology" to the purposes society designates it for.

Furthermore, Inglis overlapped with Neuberger, calling for enforcing cybersecurity by design on suppliers and manufacturers so that security is not seen as an optional afterthought.

THE JERUSALEM POST

Why did Russia's cyber warfare against Ukraine fizzle out?

The vice president of the Microsoft Threat Intelligence Center grants insight into the sudden lack of aggression from Russia at the war's outbreak.

ZACHY HENNESSEY

John Lambert, vice president of the Microsoft Threat Intelligence Center

The smart people over at Microsoft's Threat Intelligence have been keeping their eyes peeled for the latest developments in cyber warfare, and the recent activity between Russia and Ukraine has given them a lot to look at.

Speaking at Cyber Week 2022, John Lambert, vice president of the Microsoft Threat Intelligence Center, explained the lessons that his department has gleaned from observing the cyber activity between the two nations.

"Many of the actors that we track have a global remit, they're going after, you know, defense, military and intelligence diplomatic targets around the world," said Lambert.

However, the actors involved in cyber warfare against Ukraine were much more focused. "They don't have a global remit, but they focus heavily on Ukraine now but also border countries with Russia."

Russia led up to the Ukraine war with several stages of cyber attacks, composed of DDoS attacks, massive personal information leaks and wipers. "It was all about intimidation, psychological operations, all coordinating together," Lambert added.

Russia's attacks

Following the initial stage of attacks, Russia moved on to critical infrastructure attacks on government, energy and financial organizations.

"After the Olympics, we saw a much bigger destructive wave of attacks affecting over 20 organizations [in Ukraine]: hundreds and hundreds of systems wiped, heavily focused on the government and the banking sector there."

However, after the war broke out there was relative silence on the cyber front as Russia resorted to more traditional siege methods. Said Lambert: "At the beginning of the war, people were confused. Where's the big cyber? Why did they not destroy the power grid at the beginning?"

"At the beginning of the war, people were confused. Where's the big cyber? Why did they not destroy the power grid at the beginning?"

"The easiest explanation is that Russia believed in their war plans. They thought in 10 days they would be governing the country, the government would fall and they didn't want to wreck the infrastructure of the country," he said. "That did not go according to plan, and they had to adapt."

Another perspective on Russia's lack of cyber aggression during the war was offered by Professor Isaac Ben-Israel is the director of the Blavatnik Interdisciplinary Cyber Research Center at Tel Aviv University and co-founder of Cyber Week.

"If you want your capability to be adaptive, you have to invest a huge effort in maintaining this capability," he said. "Russia didn't do that, and that's why when the war started, you saw certain cyber actions, but that was the end of it."

THE JERUSALEM POST

Israel's problem: Lots of jobs, not enough workers to fill them - analysis

Unemployment is at a two-year low of 3.6%, about the same as in the United States but less than the 6.8% average in the European Union countries and the 5% rate in the OECD.

HERB KEINON

Turn on your television and you will see ads aimed at recruiting preschool teachers. Pick up a newspaper and you'll read how Israel granted permits to 3,500 Palestinians to work in manufacturing jobs. Stand on line waiting to check in at Ben-Gurion Airport and you will realize there are not enough security screeners.

Wherever you turn, you are bound to notice that Israel is facing a severe labor shortage.

Unemployment is at a two-year low of 3.6%, the exact same as in the US but less than the 6.8% average in the EU countries and the 5% rate in the OECD.

However, the employment rate, meaning the number of people in the 15-64 working-age population who are actually employed, is lower in Israel – 66.6% at the end of 2021, according to OECD statistics – than the OECD average of 67.7% and the EU average of 68.3%. In the US, the number stood at 69.4%.

Haredi men and Arab women

Israel's lower than OECD average employment rate can be attributed largely to haredi men and Arab women who are vastly underrepresented in the workforce.

Now, as the economy is getting back to full speed after the corona pandemic, what is being discovered is that there are plenty of jobs but not enough people to fill them. And this shortfall is being felt across the board in many different professions, both low- and hi-tech

In recent days, the government has announced various plans and projects aimed at easing the situation. For instance, the cabinet on Sunday approved the issuing of 3,500 permits for Palestinians to work in manufacturing and service sector positions, bringing the number of such permits up to 12,000.

Currently, 100,000 Palestinians from the West Bank and Gaza – where unemployment is at more than 25%, according to World Bank figures – have Israeli work permits, mostly for labor in agriculture or construction.

And last week, while in Morocco, Interior Minister Ayelet Shaked announced a project that would bring to Israel Moroccan construction workers and caregivers for the elderly. The Morocco World News website quoted the Histadrut's Yitzhak Moyal, who accompanied Shaked, as saying the Israeli job market can offer significant incentives to Moroccan workers, including the potential to make twice as much as the average annual salary in Morocco.

According to the website, Moyal said that Israel is looking to bring in 15,000 Moroccan construction workers that "could really improve the pace of construction in Israel."

Lack of workers in hi-tech

The lack of workers, however, is not only a problem in manufacturing, construction, healthcare and education, but is also a problem – maybe even especially a problem – in hi-tech.

In March, a Moroccan business delegation was in Israel. According to an al-Monitor report, one issue raised was for the Israeli hi-tech industry to use an abundance of Moroccan engineering graduates unable to find work in Morocco's small hi-tech sector.

Prime Minister Naftali Bennett was asked on Tuesday at Tel Aviv University's Cyber Week conference what Israel can do to relieve the urgent shortfall in hi-tech workers in the country.

Bennett said that there is "plenty of investment, plenty of everything, but we need more people," and that the country has "exhausted the immediate bucket of talent." An astounding $25.6 billion was invested in Israeli hi-tech last year, necessitating scores of engineers and programmers.

Where will workers come from?

Bennett enumerated four potential sources of workers for Israel's hi-tech industry.

The first source is haredi men, whom Bennett said are "really smart, but not inside the economy." He said getting them into hi-tech will be challenging, however, "because these folks don't know English."

He said the second pool of workers is Arab women, whom he described as "massively unemployed generally." According to Bennett, "there are lots of smart Arab women we want to bring in, and we are working on it." To do so, he added, will require the hi-tech sector to be open to "bring in folks who are different, not from the same club."

The third source is Israel's periphery in the Galilee and the Negev, which he said were "underserved," something he characterized as just "stupid policy."

And the final source of potential workers, Bennett said, is to bring in Palestinians to work in hi-tech. "I hope to see it work, that folks from Ramallah and Nablus can come. We'll see how it goes."

Microsoft senior executive Michal Braverman-Blumenstyk noted another potential source: Israelis working in hi-tech abroad. She put the number of Israeli "hi-tech people" working outside Israel at more than 150,000, and suggested appointing a coordinator to work to bring some of these people home by providing incentives.

Great idea, but to implement it, you need a government. And this illustrates yet another negative result of the country going to an election again for the third time in three-and-a-half years: it severely limits the country's ability both to plan and to implement those plans. For that, the country needs a degree of continuity in the relevant government ministries – a degree of continuity it has not enjoyed for years.

THE JERUSALEM POST

Cervello is here to protect trains from cyber threats

The company has developed a deliberate and tailored approach to railway cybersecurity.
ZACHY HENNESSEY

Cervello's co-founders (left to right): Shaked Kafzan, co-founder and CTO; Nadav Avidan, co-founder and COO; Roie Onn, co-founder and CEO.

When one pictures a hacker, the target of the hooded figure's nefarious activity is typically an unassuming citizen's bank account, a website's password database, or a high school student's grades. Cervello is a cybersecurity company focused on protecting a less-considered field: trains.

Cyber Week 2022 is currently underway, gathering hundreds of cybersecurity experts and companies to discuss the current challenges and future potential of the industry. During the event, a panel on rail security was moderated by Israel Baron, former chief information security officer of Israel Railways, and a current vice-president at Cervello. The panel was Cyber Week's first on the subject, opening the opportunity for many more niche topics to be deliberated at future iterations of the conference.

Railway mission-critical systems have long been considered secure because of their seemingly isolated network approach.

However, recent cyber attacks in Italy, Belarus and the UK have highlighted the critically vulnerable state of rail cybersecurity, as escalating global tensions coupled with industry-wide modernization have given greater motivation and new avenues for malicious actors to infiltrate vulnerable and unprotected systems.

In response to these developments, Cervello has offered rail organizations a targeted solution via their proprietary platform.

Cervello's security system passively monitors for vulnerabilities and threats across all connected infrastructure assets, providing rail operators and infrastructure managers with continuous visibility of their network and security posture, along with the intelligence and guidance they need to respond as necessary.

"Beyond feeling proud, we are truly excited to see rail cybersecurity receive the attention it deserves at such a major cybersecurity conference," said Roie Onn, CEO and co-founder of Cervello.

"Working with some of the largest rail organizations in the world, we are aware and sensitive to the needs and challenges of the industry and look forward to sharing our own knowledge and experience with other industry experts."

"Working with some of the largest rail organizations in the world, we are aware and sensitive to the needs and challenges of the industry and look forward to sharing our own knowledge and experience with other industry experts."

Roie Onn, CEO and co-founder of Cervello

As modern technology infrastructure has developed, so too has the technology used to breach it. The continuous race to protect our tech systems is fueled by an endless supply of nefarious actors who, says Nir Zuk, founder and CTO of cybersecurity company Palo Alto Networks, are pretty highly incentivized.

"It's becoming more and more prominent because we have more and more devices, and also it pays off more and more to be a cyber criminal," Zuk noted during a panel at the Jerusalem Post London Conference earlier this year. "It's very lucrative, most of the activities are being done from countries where there is no downside to being a cyber criminal."

THE JERUSALEM POST

Amid Global Push, TAU Seeks Enhanced Academic Ties in Singapore

University leadership's visit to Singapore included a special focus on new frontiers for cyber security research

A delegation of senior Tel Aviv University leadership, led by TAU President Prof. Ariel Porat, met in Singapore this week with top university and government leaders to explore new avenues for joint research collaboration in cyber security, AI, aging, climate change, medicine and other fields.

Tel Aviv University has long-held relationships with institutions in Singapore under the framework of the decades-long bilateral relations between Israel and Singapore. The countries, both recognized as world leaders in innovation and technology, have an extensive record of collaboration in R&D, commercial business, arts and culture, and beyond. The TAU delegation noted that the visit was an important step in the University's strategic focus on ramping up academic ties with leading global institutions.

Professor Porat visited Singapore to participate in the International Academic Advisory Panel (IAAP) to the Singapore Government on higher education. The presidents of other top global universities such as the University of Oxford, McGill University, Australian National University, and the University of Tokyo were among those in attendance, as well as industry leaders.

TThe TAU delegation met with leading Singaporean universities and government institutions responsible for academic research, including the National University of Singapore, Nanyang Technological University, the Cyber Security Agency of Singapore, and the National Research Foundation.

The visit focused on cyber security research collaboration, one of TAU's strengths. It came ahead of this year's Cyber Week hosted at TAU, one of Israel's largest cyber security summits. In 2015, TAU forged its first joint cyber research program with Singapore. The Blavatnik Interdisciplinary Cyber Center at TAU, a key engine of Israel's prowess in the field with over 200 researchers from different disciplines, and the Cyber Security Agency of Singapore oversee the collaboration. The program has since expanded to focus on a range of issues, including mobile app security, new anti-phishing technology, and the cyber security of smart cities.

TAU President Prof. Ariel Porat: "As Israel's top university for innovation and entrepreneurship, Tel Aviv University sees great potential in augmenting collaborations with institutions in Singapore, which is recognized as a fellow powerhouse in emerging and cutting-edge technologies."

TAU Vice President of International Collaboration Prof. Milette Shamir: "This trip represents another significant step in TAU's strategic efforts to expand academic ties in the global arena. Singapore is at the vanguard of many industrious and inspiring achievements. Together with our partners in Singapore, we look forward to driving further international collaboration to benefit students and scientific discovery."

Blavatnik Interdisciplinary Cyber Research Center CSO Dr. Yaniv Harel: "As the challenges in cyber security continue to intensify, collaboration between countries, sectors, and people is needed to safeguard the systems upon which society relies. As a global player in cyber research, we've demonstrated the joint achievements that our teams produce, and we look forward to forging new ways to solve complex cyber security issues with partners in Singapore."

BENZINGA

Israel's 12th Annual Cyber Week Highlights Unprecedented Changes in the Cyber Landscape and the Critical Need For Coordinated Response

TEL AVIV, Israel, June 29, 2022 /PRNewswire/ -- Top Israeli government figures such as Prime Minister Naftali Bennett and Defense Minister Benny Gantz, addressed the conference which is headed by Maj. Gen. (Ret.) Prof Isaac Ben-Israel, known as the "father" of the Israeli Cyber industry. Leading American and British cyber officials also contributed, including Chris Inglis the National Cyber Director at the Executive Office of the President at the White House, Anne Neurberger the Deputy Assistant to the US President and Deputy National Security Advisor for Cyber and Emerging Technologies at the White House, and Lindy Cameron CEO of the National Cyber Security Centre. Private sector leaders including Ira Winkler, Chief Security Officer for Walmart, Tim Brown CISO of SolarWinds, Jane Horvath, Chief Privacy Officer of Apple, Jason Chan, Former VP of Information Security at Netflix, also addressed the conference. Supported by Israel's Ministry of Economy and Innovation, attendees joined from over 80 countries from all over the world. Guests included startups and major investors, together with numerous sponsors, and partners.

Cyber Week is jointly held by the Blavatnik Interdisciplinary Cyber Research Center (ICRC); The Yuval Ne'eman Workshop for Science, Technology and Security at Tel Aviv University; and the Israeli National Cyber Directorate under the Prime Minister's Office. The gathering occurred against the backdrop of unprecedented cyber challenges and events including Russia's war on Ukraine. Speakers described a dramatic and concerning rise in cyber warfare as well as cybercrime - cyber-related damage is predicted to hit $10.5 trillion annually by 2025, while cybersecurity spending on data protection and risk management could reach $172 billion globally in 2022. Yet they also expressed hope in the effectiveness of properly implemented defenses and evolution in defensive cyber techniques to meet the challenge.

Israel's Prime Minister Naftali Bennett pointed out how "inevitably cyber is going to become one if not the most prominent dimensions of future warfare," while drawing attention to the vital need for global collaboration in the cyber sphere saying, "In cyber it's [collaboration] vital because the same bad guys who are attacking one company or country are attacking others at the same time. If you can share that information everyone else can defend themselves. It's like a pickpocket in a subway and if someone sprays them with red paint everyone can see and defend themselves."

Chief Market Strategist, Matt Maley, has just released his latest pick, and investing in this company could be like buying Amazon stock in 2017. Click Here before it's too late!

Ira Winkler: CISSP, Chief Security Architect, Walmart outlined the important role government plays saying,

"at a high level, governance tells people how to do things correctly with cyber security at the forefront." He also recognized the need to account for the human aspect of cyber and to be realistic when devising and implementing strategy, "A user is as much as part of the system as a computer. Stop expecting people not to click on suspicious content, but rather have a strong network protecting them."

Israel's Minister of Defense, Benny Gantz, outlined the increasing shift of conflict to the cybersphere and that bad actors are already carrying out attacks via cyber, particularly Iran. The country uses "new [cyber] proxies [who] "are terrorists with keyboards," in addition to their direct actions. In response, Defense Minister Gantz stressed the need for private companies to follow government guidelines and cooperate saying, "Iran is first a global challenge, then it is a regional challenge, and only finally is it a threat to the State of Israel. The same goes for the cyber dimensions and the same framework of cooperation vis-a-vis Iran is expanding to cyber."

About CyberWeek:

Cyber Week is a leading international cybersecurity event that provides a unique opportunity for experts from industry, government, military and academia to share their knowledge about the challenges and opportunities in the field. Cyber Week is hosted by the Blavatnik Interdisciplinary Cyber Research Center and the Yuval Ne'eman Workshop for Science, Technology, and Security, at Tel Aviv University, headed by Major Gen. (Ret.) Prof. Isaac Ben-Israel together with the National Cyber Directorate at the Prime Minister's Office, The Ministry of Economy and Industry, and the Ministry of Foreign Affairs.

the algemeiner

Bayer to Establish Cybersecurity Hub in Israel

JNS.org – Pharma giant Bayer has announced plans to establish a cybersecurity hub in Israel, which will be integrated into Bayer's global cyber unit and will be one of the largest internal units of this kind in the company.

A delegation of top Bayer executives arrived in Israel on June 26 for a three-day visit, meeting with Economy and Industry Ministry Director-General Ron Malka to discuss the German company's plans to deep-dive into the Israeli market.

The delegation included, among others, Bijoy Sagar, Bayer's chief information technology and digital transformation officer, and Gary Harbison, head of cybersecurity and risk management, who were the driving force behind the move. The two also spoke at the main plenary of Cyber Week 2022, the annual international cybersecurity expo hosted by Tel Aviv University.

"I am excited by the spirit of innovation, level of talent and pragmatism I witnessed in the start-up ecosystem, the government and universities in Israel in the sphere of information technology," said Sagar. "Bayer business in Israel is strong and the cybersecurity hub is another great addition to our initiatives in Israel."

During Cyber Week, top TAU and Bayer executives also inked a cooperation agreement to promote groundbreaking cybersecurity research from Tel Aviv University.

"As a company engaged in R&D in the core areas of life sciences, the ability to integrate with Israel's unique cybersecurity ecosystem, alongside sectors such as medical innovation and agricultural development is an opportunity to integrate as players in the Israeli market and provide added value for Bayer and for the ecosystem," said Hugo Hagen, managing director of Bayer Israel.

"As a Norwegian who has worked in Israel for three years, I feel a mission to promote Israel on Bayer's investment map and to strengthen the company's position within Israel, as well as that of the Israeli headquarters within the global headquarters," said Hagen.

"The ecosystem here is impressive and it would be a mistake not to try to enjoy the possibilities that exist here, and of course, I am proud that the decision was made to establish the new cyber security unit here," he added.

"There is no doubt that such initiatives contribute to employment, innovation and Israel's image, and attract other international investments," noted Malka. "We will continue to represent the best Israeli innovation has to offer and link it to leading companies. We welcome Bayer's expansion in Israel and we are working to develop future similar initiatives."

Yael Mor, who will run the hub for Bayer, said, "It is exciting to create something the activities of which will have an impact in the world beyond Israel's borders. Along with our focus on the cyber unit, we will engage in locating Israeli innovation in cyber security."

Bayer is one of the largest pharmaceutical and life sciences conglomerates in the world. Its main areas of business include consumer healthcare products, agricultural chemicals, and seeds and biotechnology products. The company set up its offices in Israel in 2008 and currently employs 150. Worldwide, Bayer maintains a presence in 83 countries, employing some 100,000 people.

HAARETZ

Bennett Calls for Integration of Palestinians Into Israeli Tech Sector

Speaking at Tel Aviv University's Cyber Week, Israel's outgoing PM also predicted a significant widening of the role of cyberwar, stating that he was 'surprised by the [relative] lack of cyber tools in the war in Ukraine'

Sam Sokol

Prime Minister Naftali Bennett reiterated his desire for the integration of Palestinians and other marginalized groups into the Israeli technology workforce on Tuesday, saying that Israel has "exhausted" its available "bucket of talent."

"We need just more good people," the former technology CEO told attendees at Tel Aviv University's annual Cyber Week.

"I gave an approval, an official approval and the government approved the immediate joining of Palestinian employees in Israeli high-tech, including free movement from the PA [Palestinian Authority] here, and I hope to see it work. I think, folks from Ramallah or Nablus, or whatever, should come, we'll see how it goes."

Last November, Bennett's government approved a plan to employ Palestinian workers in Israel's high-tech sector. The plan, which was set to be implemented over three years, includes a quota of up to 500 Palestinian workers, similar to quotas for other industries, and the employees will be able to work from Israel if required. The quota set in the plan is small compared to the number of Palestinians already working in Israeli high-tech.

Not Even 500 Palestinians in Israeli High-tech Can Hide the Exploitation

These Arabs Are Fighting the Old Boys Club of Israeli Hi-tech

Israel foiled 1,500 hacking attempts this year, cyber chief says

Under the plan, these workers will have to earn a wage of no less than 150 percent of the average salary in Israel. Such a quota will not completely solve the tech worker shortage currently facing Israeli high-tech, but the plan is expected to whet the appetite of Israeli employers, as well as helping to advance the ailing Palestinian economy.

By enlisting ultra-Orthodox men, Arab women, residents of the periphery and Palestinians into the tech sector, "we can unleash another wave of talent and growth in Israel," Bennett said.

Turning to his tenure as prime minister heading the country's most diverse coalition to date, which only lasted a year, Bennett said that Israelis had learned that while "we all tend to have prejudices of folks with different opinions," it "turns out that they are very nice folks."

"When there's decent people and good people we can all work together for the betterment of Israel. That's the single biggest achievement of this government."

Bennett also addressed the tech sector's role in modern conflict, predicting a significant widening of the role of cyberwar, though noting he was "surprised by the [relative] lack of cyber tools in the war in Ukraine. I thought it would be much more advanced."

"Today you can get stuff done hitting your enemy through cyber, which in the past would require to covertly send 50-100 commando soldiers behind enemy lines with huge risk, and now you can get a bunch of smart folks sitting behind a keyboard with the same effect, which is why inevitably cyber is going to become one of the most prominent dimensions of future warfare. It just makes sense," he said.

"On the geopolitical level we're going to see a lot of investment across the world in cyber offense and that's on a global level and obviously the same applies to crime."

Likely responding to media reports of recent Israeli strikes against targets within Iran, Bennett said that Israel is "doing pretty well on the defensive side."

"My approach with our enemies, especially Iran, we don't go around just wrecking havoc in Tehran. That's never been our policy. But our policy is if you mess with Israel you'll pay a price and you can no longer hit Israel through proxies and get away with it. We're not going to try and fight those folks but hit the bully."

In addition to Bennett's remarks, Gabi Portnoy, head of the National Cyber Directorate, also said during the conference that Iran has become a key player in cyberspace, along with Hamas and Hezbollah. "We see them, we know how they work and we are there," adding that Israel has blocked about 1,500 cyberattacks in the past year.

Omri Zerachovitz contributed to this report.

HAARETZ

If the Iranians Are Cyberterrorists, So Are Israelis

Defense Minister Benny Gantz owns the copyright to a new term: cyberterrorism. In a speech last Wednesday at Cyber Week, an annual international cybersecurity conference held at Tel Aviv University, he said "Iran is leading cyberterrorism." He also added a threat, as though the frequent threats by Israel's leaders, the IDF chief of staff and the head of the Mossad are insufficient: "Iran operates proxies in the cyber dimension as well. The new proxies are terrorists with a keyboard, who will be punished like other fighters in terrorist organizations."

Sam Sokol

'This president loves Israel:' U.S. ambassador talks Biden visit, ties with Saudi Arabia

There is seemingly no limit to Israel's desire to use the word "terror," which took root in the Reign of Terror masterminded during the French Revolution by Maximilian Robespierre. With time the word took on the meaning of using violence, mainly against civilians, in order to create a climate of fear to achieve a political, military or personal goal. That's terms like "acts of terror" and "terror attacks" entered the lexicon.

Since Israelis in general and the political and military leadership in particular are in love with the word because it reinforces paranoia and victimhood, absurd derivatives have been added to ordinary terrorism: "diplomatic terrorism" and "legal terrorism." They aim to deny the Palestinians the right to fight the occupation with diplomatic tools – to pressure or influence states to change their attitude toward Israel – or legal tools – to sue members of the Israeli military in the International Criminal Court. But these Palestinian efforts are not terrorism. They are its exact opposite. Someone who uses diplomatic or legal means, or even calls for a boycott against Israel, is not a terrorist. He is a diplomat or a legal scholar or a BDS activist, who actually refrains from terrorist activities.

Nor is the use of digital tools terrorism. It is a means, increasingly common in recent years, of achieving a large variety of goals. It helps criminals commit economic offenses such as monetary theft, fraud and sex crimes; it enables identity theft, impersonation and information theft. Cyber tools enable the dissemination of disinformation in an effort to distort reality and create "alternative truths." They can influence public awareness in order to try to change election results, as Russian President Vladimir Putin tried to do in the 2016 elections in the United States, Britain, France and other Western democracies.

In the military and security context cyber must be discussed in terms of warfare rather than terrorism. Since World War I, war has been waged in three dimensions: on land, on sea and in the air. Less than 20 years ago the cybernetic dimension began to develop, and now another dimension has been added – artificial intelligence.

The potential damage to the enemy through cyberwarfare is tremendous. It can cause the deaths of hundreds of thousands of people. If hospital computer systems are paralyzed, people will die. Instead of firing a missile at a power station, they hack its computers. If a nuclear power plant is shut down, it may emit radioactive fallout. If computers operating dams are interfered with, there will be flooding. If water companies' computers are disabled, water sources can be poisoned, as the deputy commander of the IDF Military Intelligence Unit 8200 revealed last week during Cyber Week.

There is a reason why the U.S. president's authority to order cyberwarfare against an enemy state is based on their authority to activate nuclear weapons. The damage from cyberwarfare can resemble that resulting from dropping a nuclear bomb, with one difference: Cyberwarfare leaves no traces. This is a war that is hidden from the eye, creating a gap for plausible deniability.

Israel and the United States (followed by China and Russia) were among the first countries in the world to understand that. Both were also the first to develop far-reaching technological capabilities. Israel's Unit 8200 and the U.S.'s National Security Agency and the Cyber Command used cyberwarfare against Iran. This was in 2008-09, when the Stuxnet virus was introduced into the computers operating the centrifuges at the uranium enrichment facility in Natanz. The "poisoning" of the computers damaged one-third of Iran's centrifuges. Since then Israel has improved its capabilities; computers in army bases, crucial civilian infrastructure and other facilities in Iran are being bombarded by cyberattacks attributed to the Mossad and Unit 8200. The movement of ships to the Bandar Abbas port was stopped, as was the operation of gas stations and train stations. Last week there was a report of serious damage to three steel manufacturing plants serving Iran's Revolutionary Guards.

When Iran realized that Israel and the United States were waging cyberwarfare against it, Tehran began to respond. U.S. banks were hit, as were computers of the Saudi oil company Aramco. Not a day goes by that Iran doesn't attack Israel, although with very little success.

If what Iran is doing is terrorism, Israel's activities are also terrorism. That's why it is hypocrisy on Gantz's part to accuse Iran of cyberterrorism. Such statements are nonsense, and we would do well not to demonize our rival. After all, a clandestine war between Iran and Israel has been ongoing for about 20 years using all available tools, including cyberwarfare.

ynet ידיעות אחרונות

'If you mess with Israel, you pay a price,' says Bennett in message to Iran

Speaking at TAU's cyber week, outgoing premier says Israel never seeks to 'create destruction and terror,' but will not allow its enemies to harm it without a response; adds cyber will be 'most prominent area of combat in future'
Nina Fox

Prime Minister Naftali Bennett said Tuesday that when it comes to the Iranian threat, the government's policy remains the same as with any other enemy, adding that "if you mess with Israel, you pay a price".

Speaking at a conference marking the start of the annual cyber week at Tel Aviv University, the premier said, "my attitude in general when it comes to our enemies - especially Iran - is that we do not work to create destruction and terror, this has never been our policy."

"My policy is that if you mess with Israel - you will pay a price. You will not be able to harm Israel through proxies, Hezbollah or Hamas, thinking you can get away with it."

He added that in today's world it's no longer necessary to send "100-50 commandos behind enemy lines" to inflict damage on adversaries. "Today it is possible to do things - harm the enemy - through cyber warfare.

"Now, all you need is a few people and a keyboard. In the end, cyber will become the most prominent area of combat in the future."

He added: "I am quite surprised by the shortage, or relative shortage, of cyber tools used in the Ukraine war. At the geopolitical level, we see a lot of investment around the world in cyber attacks."

He also acknowledged recent cyber attacks on civilian infrastructure in Israel, saying, "At the end of the day, companies have a personal responsibility that they must take on. If our customers' information is hacked, it's the companies' problem [to deal with].

"At the national level, Israel's cyber defense system works with companies to help them defend themselves. Just as there is nuclear deterrence, there will be cyber deterrence. "

ynet ידיעות אחרונות

State Comptroller says Israeli elections aren't properly guarded against cyberthreats

Tova Zimuki

Israel's State Comptroller said Wednesday elections in the country are not adequately protected against cyberattacks.

Speaking at a cyber conference at Tel-Aviv University, Matanyahu Engelman said said there were "major deficiencies in readiness for cyber attacks in Israel's Central Election Committee."

He added: "We're exposed, our data is exposed to too many people, our economy, children, health and security are all exposed."

Cyber Week
June 27th-30th, 2022
Tel Aviv University, Israel
Yuval Ne'eman Workshop for Science, Technology and Security Tel Aviv University
ICRC Blavatnik Interdisciplinary Cyber Research Center
TEL AVIV UNIVERSITY אוניברסיטת תל אביב
Cyber Israel National Cyber Directorate
In cooperation with:
Ministry of Foreign Affairs Israel
ISRAEL CYBER ALLIANCE
State of Israel Ministry of Economy and Industry Foreign Trade Administration
ISRAEL EXPORT INSTITUTE

nocamels

'Leading Cyber Ladies' Help Empower Women In The Cybersecurity Sector

Simona Shemer

Women account for 50 percent of the population, but they make up only about 28 percent of the cybersecurity industry, according to Keren Elazari, Israeli security researcher and industry analyst who tells NoCamels she has always encountered her fair share of unfavorable comments about how she was able to keep up with a male-dominated industry

"I was at a tech security conference this week and I had people coming up to me, people that are maybe half my age, questioning whether I had a computer science degree. I answered, yeah, 20 years ago, please don't give me an exam on infinite decimal math right now, because when I was studying it, you were still in kindergarten."

This is just one of the reasons Elazari, a noted public speaker whose popular 2014 TED talk helped shape the global conversation about the role of hackers and the evolution of cybersecurity, helped form Leading Cyber Ladies, a global movement of top women in cyber tech coming together to talk trends, network, and provide support and resource to each other in a comfortable and professional environment.

"What we're trying to achieve with leading cyber ladies, is to really increase that impact and the visibility of women in cybersecurity, because we believe through role models, through networking, through shared experiences, we can increase the impact of women in cybersecurity and getting more women into our field and into our communities. That's our goal. That's our mission statement. And we started here in Israel. But we now have grown globally, and we have chapters around the world. And even today, our Israeli community is our biggest community," says Elazari.

The network, which now has chapters in Japan, Canada, New York, and UK, began its first chapter in Tel Aviv in January 2015 with just 30 women. Today, there are around 3,000 globally, with over 1,000 in Israel. The first meetup was the idea of Hila Meller, a cybersecurity expert and executive of CA Europe at the time, who is now the Vice President for telecom giant BT Security. Meller suggested the idea to Elazari and together they set up the meeting with speakers that included El Al Airline's chief information security officer and the leading digital crimes prosecutor in Israel, among others.

"We called ourselves the 'Leading Cyber Ladies,' since we want to inspire others and lead more diversity and equality in our industry," the group's official website says, "We felt it represented our commitment to lead for this change to happen."

Israeli incident response and security expert Reut Menashe, who is also the founder and CEO of Tetrisponse, an incident response consultancy firm, tells NoCamels she joined Leading Cyber Ladies in 2017, to become part of an enriching community in her field and help it expand worldwide.

"I believe in the purpose. I am in information security for a number of years. I know what it's like to be a woman in this world," she continues, "Karen and Hila understood that there must be this community in order to empower women in cybersecurity and I joined to help and support."

Menashe is also one of the organizers of BsidesTLV, a security research community event in Israel, taking place during Tel Aviv University's Cyber Week.

She says the 'Leading Cyber Ladies' network began to expand because women in the field from around the world would come to Israel for cybersecurity or tech events and someone would invite them to come to speak at the meetings or meet the other women. Elazari and Menashe also participate in and present at many international events and will always talk up their network.

Elazari, who calls Menashe her co-pilot, is quick to different kinds of women that have become part of the group over the years. "We've had the cybersecurity managers of Israeli airlines. We've had women from Israeli banks. We've had women from innovative startups and founders of innovative cybersecurity startups. and omen who are leading teams of dozens if not hundreds of people," she explains, "These are women that are already really successful, but they are constantly tested and judged. We wanted to put the emphasis on leading."

"This week, I got a request from someone in Africa that wants to start a group," Elazari continues, "This person heard me speak through a virtual conference in Nigeria and had the idea then and now they finally have a plan how to do it. Women are really interested in organizing and it's easier for them when they hear there's already a movement and a network. It's an opportunity to be part of something."

Becoming visible

Elazari says that based on her own experience, women in the cybersecurity industry were never as visible as they should have been for a variety of reasons. They were not connected to one another. They would not go to conferences or give talks because they were not comfortable or because they were women, they had to prove themselves five

Cyber Week
June 27th-30th, 2022
Tel Aviv University, Israel
Yuval Ne'eman Workshop for Science, Technology and Security Tel Aviv University
Blavatnik Interdisciplinary Cyber Research Center
TEL AVIV UNIVERSITY אוניברסיטת תל אביב
Cyber Israel National Cyber Directorate
In cooperation with:
Ministry of Foreign Affairs Israel
ISRAEL CYBER ALLIANCE
State of Israel Ministry of Economy and Industry Foreign Trade Administration
ISRAEL EXPORT INSTITUTE

or 10 times over.

"When I first got started, more than 25 years ago, I was easily the only woman at a hacker conference or a security conference or at the meeting table or on my team at a technology company. I was really used to being the only woman around. We are proud to see it changing. There are more and more women around and in fact, the industry surveys that look at the global cybersecurity workforce here in Israel and around the world say that the numbers are getting higher and higher," Elazari says.

Reut Menashe, a co-creator at Leading Cyber Ladies

Indeed, the cybersecurity community, particularly in Israel, is making greater efforts to make sure women are part of the conversation. This year's Cybertech Global 2022 conference in Tel Aviv included a panel devoted to cyber tech women and opportunities in cybersecurity for underrepresented sectors in the industry featuring female representatives from Israeli DevOps automation software company JFrog, authorization and identity management solutions firm PlainID, AliceCode, an Israeli initiative teaching young girls how to code, and many more. Ruth Shoham, CEO of The Open University of Israel also spoke about leading women in cybersecurity.

On International Women's Day, the Israel National Cyber Directorate sent out a list of prominent female experts in the cybersecurity industry with the intention of increasing female representation in public appearances. The list, which can be found here in Hebrew, includes names like Yuval Lazar, a senior security researcher at automated penetration testing firm Pentera, Sivan Ashkenazi, a cloud security specialist at Deloitte, and Einat Meyron, a cyber resilience specialist.

For their part, the Israeli chapter of 'Leading Cyber Ladies' is empowering young women with aspiring cybersecurity careers through mentorships, connecting them with other women that are already leading the field and have established themselves in the sector. The group also runs events, like Capture The Flag, a competition that Elazari says is very common in the cybersecurity world, but "you don't see a lot of women compete."

The Leading Cyber Ladies are also very connected to each other in the world of social media, Menashe and Elazari tell NoCamels, pointing to groups on What's App, Facebook, LinkedIn, and Instagram. It's a way for women in cybersecurity to connect at events, even when they don't know each other, because they're part of the same group, Elazari says.

Elazari also says the team in Israel works very hard to provide professional development opportunities to the community, like help for studying for specific exams, organizing product pitch events, and providing information on how to get certain certifications. "We also spend 30 percent of our time if not more supporting our global network come up with ideas for events and content," says Menashe says, "And we are always looking for more women to join the team!" she adds.

The events aren't even limited to women, she adds "We do invite women to our meetups, but we also invite men. Change cannot come only from women. The change depends on everyone. Obviously, if most of the companies are being managed by men then the change needs to come from them. So it's important to understand that we are in it together. And I believe we are allies."

nocamels

Israel's Annual Cyber Week Returns To Tel Aviv University Next Week

Max Kaplan-Zantopp

The annual international cybersecurity summit Cyber Week, will return to its in-person format next week beginning Monday, June 27 at Tel Aviv University.

Over the past 12 years, Cyber Week has become one of the world's most recognized international cybersecurity events, providing unique platforms for experts to share their knowledge regarding the challenges and opportunities in the field.

The event will be hosted by the Blavatnik Interdisciplinary Cyber Research Center and the Yuval Ne'eman Workshop for Science, Technology and Security.

Events will run for a full week and include over 40 roundtables, panels, workshops, forums, training sessions, competitions, and more.

Thousands of attendees including cybersecurity experts, industry leaders, startups, investors, academics, diplomats, and government officials from more than 80 countries are expected to arrive.

The 12th Annual International Cybersecurity Conference, the biggest and most highly anticipated event of Cyber Week every year, will be held from June 28-29. Some of the most renowned names in the cyber world will discuss crucial dilemmas and unsolved problems facing the public and private sectors of every company, city, and country in the modern world.

Among this year's confirmed speakers are Prime Minister of Israel Naftali Bennett; Israel Minister of Defense Benjamin Gantz; Deputy Assistant to the President and Deputy National Security Advisor for Cyber & Emerging Technologies, White House, USA Anne Neuberger; National Cyber Director of the Executive Office of the US President Chris Inglis; the Director General of the Israel National Cyber Directorate Gaby Portnoy; Conference Chairman of Cyber Week and Director of Blavatnik Interdisciplinary Cyber Research Center at the Tel Aviv University Maj. Gen. (Ret.) Prof. Isaac Ben-Israel; Chief Privacy Officer of Apple, Inc. Jane Horvath; CEO of the National Cyber Security Center Lindy Cameron; CISO of SolarWinds Tim Brown; Founder of action:reaction and Netflix-star of Tinder Swindler Cecilie Fjellhøy; and Former VP, Information Security of Netflix Jason Chan.

"Cyber is an increasingly vulnerable space that is affecting everyone," said Prof Isaac Ben-Israel. "Businesses must wise up to the real and growing threat of cyber attacks, and cybersecurity experts must be ready to respond to the escalating demand for cyber security with novel solutions. We must prepare now to be ready for what we know tomorrow will inevitably hold."

nocamels

Tel Aviv University Leaders Explore Academic Ties In Singapore

Isabel Engel

Tel Aviv University leaders met with top university and government representatives in Singapore this week to explore potential research collaborations in fields of cybersecurity, AI, aging, climate change, medicine, and more.

The team at Tel Aviv University (TAU) – led by TAU President Professor Ariel Porat – aimed to build off of long-standing relationships with institutions in Singapore and decades-long bilateral relations between Israel and Singapore. Both Israel and Singapore are leading nations in innovation and technology, with extensive collaboration in fields including R&D, arts and culture, and commercial business. The TAU delegation noted that the visit was an important step in the University's growing focus on academic ties with top global institutions.

"As Israel's top university for innovation and entrepreneurship, Tel Aviv University sees great potential in augmenting collaborations with institutions in Singapore, which is recognized as a fellow powerhouse in emerging and cutting-edge technologies," said TAU President Professor Ariel Porat.

Professor Porat visited Singapore to partake in the International Academic Advisory Panel (IAAP) to the Singapore Government on higher education. He was joined by industry leaders and presidents of other leading global universities, including the University of Oxford, McGill University, Australian National University, and the University of Tokyo. The TAU delegation team met with several Singaporean universities and governmental institutions including the National University of Singapore, Nanyang Technological University, the Cyber Security Agency of Singapore, and the National Research Foundation.

The visit placed a premium on cybersecurity research ahead of TAU's Cyber Week event, one of Israel's largest cybersecurity summits. The Blavatnik Interdisciplinary Cyber Center at TAU – a key engine of Israeli cybersecurity with over 200 researchers – has overseen collaboration between TAU and Singapore since it was initiated in 2015.

"As the challenges in cyber security continue to intensify, collaboration between countries, sectors, and people are needed to safeguard the systems upon which society relies. As a global player in cyber research, we've demonstrated the joint achievements that our teams produce, and we look forward to forging new ways to solve complex cyber security issues with partners in Singapore," said Blavatnik Interdisciplinary Cyber Research Center CSO Dr. Yaniv Harel.

nocamels

Pharma Giant Bayer To Launch Cybersecurity Hub In Israel

Isabel Engel

Global pharmaceutical giant company Bayer announced last week that it would establish a cybersecurity hub in Israel.

The German multinational pharmaceutical and life sciences corporation will be one of the largest internal cyber units of a global company operating in Israel. The company will incorporate the hub into Bayer's global cyber units.

By establishing a cyber branch in Israel, Bayer will be uniquely positioned to bring added value to Israeli business and local operating pharmaceutical companies. Additionally, the company will be able to connect Israeli businesses to its global operations in the fields of health, agriculture, and innovation.

"As a company engaged in R&D in the core areas of life sciences, the ability to integrate with Israel's unique cybersecurity ecosystem, alongside sectors such as medical innovation and agricultural development is an opportunity to integrate as players in the Israeli market and provide added value for Bayer and for the ecosystem," said Hugo Hagen, managing director Bayer Israel.

"As a Norwegian who has worked in Israel for three years, I feel a mission to promote Israel on Bayer's investment map, and to strengthen the company's position within Israel, and of the Israeli headquarters within the global headquarters. The ecosystem here is impressive and it would be a mistake not to try to enjoy the possibilities that exist here, and of course, I am proud that the decision was made to establish the new cyber security unit here," Hagen continued.

Several global Bayer executives came to Israel last week to explore the Israeli market and overall business environment in light of the Hub establishment. The delegation brought many Bayer leaders to the Startup Nation, including Bijoy Sagar, Chief Info. & Digital Transformation Officer; Gary Harbison, SVP CISO Head Cyber Security & Risk Management; Saskia Steinacker, SVP Strategy & Digital Transformation; Jeanne Kehren, CIO Pharma; Chris Sawall, Bayer Crop Science ISO & Head of Digital Security Services; Martin Bartel, Executive Management Support.

Two of these leaders, Sagar and Harbison, spoke at the Main Plenary of Tel Aviv University's (TAU) Cyber Week at the end of June. Cyber Week, a large international cybersecurity event hosted each year, serves as a hub for cybersecurity innovation in Israel. At the event, several senior Bayer executives met with Israeli professionals – including the CEO of TAU's technology transfer company, Ramot, Keren Primor Cohen, and Head of TAU's Blavatnik Interdisciplinary Cyber Studies Professor Isaac Ben-Israel – to sign a cooperation agreement to promote groundbreaking cybersecurity research at TAU. By partnering with industry-leading companies like Bayer, Ramot is working to bolster TAU innovation and research.

National Cyber Security Centre

Lindy Cameron speech at Tel Aviv Cyber Week

The CEO of the NCSC emphasises the ties between academia, industry and government in countering cyber threats.

Good morning everyone. And it's fantastic to be here again in Tel Aviv.

Thank you so much for inviting me. And thanks to those of you who are joining us online - thanks for tuning in. It's great to be back here for a 2nd year running despite the challenges of COVID.

I would like to start by congratulating Gaby Portnoy on his appointment as Director General of the Israel National Cyber Directorate earlier this year.

My own organisation - the UK's National Cyber Security Centre - and the INCD share an awful lot in terms of mission and of outlook.

Our collaborations over the years have really delivered and I look forward to expanding the partnership in the years ahead.

Since I was here in Tel Aviv this time last year, the brutal Russian invasion of Ukraine has not only changed the geo-political landscape but transformed the context for our work on cyber security.

When the first Russian tank crossed into Ukrainian territory, the unthinkable suddenly became a terrifying reality.

Millions of innocent people have had their lives, homes and families taken from them.

And while Russia inflicted this physical oppression, they were also conducting a cyber campaign. This came as no surprise. Russia has consistently used cyber pressure to stress its rivals, distract them, and where possible disable them.

But – just as they have done on the battlefield – Ukrainian cyber defenders have done an incredible job of repelling many of these attacks. They are real heroes.

And I think resilience and preparation are at the heart of this success. I'll come back to this point shortly.

But for all the pernicious activity that we have seen from Russia in the last few months in cyber space and beyond, we must not lose sight of the longer-term strategic challenges posed by the continued growth of China as a technological and economic power.

Because in cyber security this challenge is particularly acute because of the globalised nature of digital technology.

The Chinese government's use of technology is about coercion and control. And the country's technological and economic power mean they can export this vision very widely.

Once the world relies on technology delivered with an authoritarian bias, it will constrain our choices.

As allies...as equals...our more open systems can take time to reach agreement. And when we leave important choices unmade, we leave gaps in our defences which will be rapidly exploited.

So these challenges - from China, Russia and others - make it impossible for us to leave cyber security for another day.

So now is the time to innovate, educate and empower our citizens.

The democracies of the world have to challenge themselves to develop technologies and systems which allow us to avoid reliance on products not aligned with our values.

And I hope that the 'start-up nation' of Israel can play an important role in this innovation over the years to come.

But – even with a war raging in Ukraine – the biggest global cyber threat we still face is ransomware.

That tells you something of the scale of the problem.

Ransomware attacks strike hard and fast. They are evolving rapidly, they are all-pervasive, they're increasingly offered by gangs as a service, lowering the bar for entry into cyber crime.

And that's what makes them such a threat – not just the nationally significant incidents that my team and I deal with in the NCSC, but also the hundreds of incidents we see that affect the UK more widely every year.

These complex attacks have the potential to affect our societies and economies significantly, if it were not for the expertise of our incident management operators working in collaboration with their counterparts in industry and their international counterparts gathered here today.

So, we worked hard over the last year, to really understand, with our law enforcement partners, the criminal system behind ransomware. We want to drive down profits and drive up the risk to the criminals. We continue to work on understanding the scale, nature and evolution of their techniques.

We want to make ransomware an unprofitable and unattractive business.

Russia may dominate the headlines at the moment, but this threat of ransomware has not gone away – and nor have we stopped our relentless focus on it.

But it's not all doom and gloom.

I've mentioned Ukraine, and closer to home, just look at the work undertaken by our hosts here in Israel - a shining example of what can be done when a nation takes cyber security seriously.

The technology developed here is truly world class. The talent in the cyber security sector is second to none. And your defences are some of the strongest in the world.

But making the most of our digital future is too big an issue for any one nation to handle alone.

Whether its drip feed irrigation or health and climate tech, Israel has always been proud to innovate for the benefit of people, well beyond your borders.

So, I hope you will continue to produce cyber security solutions which are safe, strong and affordable for the whole world.

Because an isolationist stance is just not going to work, long term. I think the war in Ukraine is a case in point there.

Technology and tactics developed there won't remain local problems. We've all watched that carefully.

An important part of our response to this as an international community is a clearer definition and enforcement of the rules that govern activity in cyberspace.

If we are to ensure that the digital world remains a place of opportunity, and to avoid it becoming a place of conflict and struggle, we must be clearer about the guidelines and norms that transcend international borders. We must explore innovative new technologies and share lessons learnt.

Last month, the UK's Attorney-General set out the UK views on how international law applies in cyberspace in peace time.

She focused on providing more detail on the rule on prohibited intervention. Her speech brings this to life by providing examples from key sectors of the sort of cyber behaviour that would be unlawful if conducted in peacetime.

She stressed that the United Kingdom's aim is to ensure that future frontiers evolve in a way that reflects our democratic values and interests, as well as those of our allies.

We need clarity on the points of law if they are to be part of a framework for governing international relations and if they are to rein in irresponsible cyber behaviour.

Another very significant element is the international regulation of sophisticated cyber capabilities. Some of which have been pioneered here, in Israel.

If we're going to maintain a cyberspace which is a safe and prosperous place for everyone, it is vital that such capabilities are produced and used in a way that is legal, responsible and proportionate.

I am delighted that Israel has tightened export controls around these tools, making it far more difficult for nations with concerning records on privacy and human rights to acquire such intrusive spyware.

It is really important that every actor, from the developer to the end-user of these types of technology and capability acts responsibly, with appropriate safeguards to protect against misuse.

There is a key role here for those of you in the private sector, for our respective cyber industries and technology companies in conducting due diligence and ensuring their products are not deployed in a manner that creates harm or undermines these principles.

One of the great benefits of coming to fantastic events like this at Tel Aviv Cyber Week is the opportunity to learn from others and exchange ideas.

In the UK, we take our 'whole of society' approach to cyber security really seriously. We want everyone 'on the team', pulling together to present a cohesive and resilient digital face to the world. Every citizen, business and utility, every school, charity and hospital. And I think that is something that we look to you for some real lessons on.

We want to help create a society that is resilient to cyber attacks, where cyber security is second nature to all of us.

Israel is already some way ahead in this process. Your cyber security ecosystem of businesses, education, and research is thoroughly inspirational. I am personally in awe of your cyber education programme – it is something that the UK's CyberFirst scheme has learnt many lessons from.

And I appreciate that building this kind of depth of understanding, as Professor Ben-Israel said, takes time. But early investment really pays dividends.

The same is true of organisations around the world as they build resilience to cyber compromises.

Which is why my organisation has been encouraging organisations throughout the UK to follow the advice that we give as NCSC to improve their resilience – learning from the lessons we've seen in Ukraine of how to build that resilience in the face of the Russian onslaught.

And learning the lessons of Ukrainian cyber security in recent months has been something we've tried to help our companies in the UK to understand.

But to build this kind of resilience we need to create an environment where people are not too busy putting out the little fires to focus on the longer term.

Which is why the NCSC is really proud of our Active Cyber Defence programme, which helps to reduce the volume of low-level commodity attacks. And we've had some noteworthy successes.

Our 'Takedown project', for example, removed 3.1 million malicious URLs in 2021. Which we think saved the UK £223 million.

In the same period, our 'Protective DNS' service handled more than 600 billion requests. 160 million of which were blocked from accessing known sources of malicious content.

And, one service that I am particularly proud of is our Suspicious Email Reporting Service, because we enlist the great British public to help us. So far, the public have told us about 10.5 million suspicious emails, from which we've taken down 76,000 online scams. It's a great example of our "whole of society" approach in action and it helps our citizens feel as if they're helping us as a country, not just to protect themselves, but to protect the nation as a whole.

So, this ambitious approach to a whole of society approach to cyber. But I think to succeed, partnerships are essential. So, we are building stronger ties between academia, industry and government.

We're reaching out to startups, with initiatives designed to spur the development of tools which will protect the UK's smaller and medium sized businesses.

And we are engaging, as we are here, with our friends and allies.

We must come together around our shared values. Each nation bringing its own particular skills and strengths to build a network which is naturally resilient to attack, one which favours innovation, discourse and creativity over control and coercion.

They are big challenges, and they point to even larger actions. So, I look forward to discussing them with you here at Cyber Week, and in the months and years to come.

Thank you for your time.

National Cyber Security Centre

Commercial cyber capabilities must be used legally and responsibly, says UK NCSC CEO

Lindy Cameron's speech at Tel Aviv Cyber Week emphasised the importance of partnerships and international regulation of sophisticated cyber capabilities.

The head of the UK's National Cyber Security Centre (NCSC) has delivered an international speech emphasising the importance of legal and responsible use of commercial cyber capabilities.

Speaking to an audience at the globally prestigious Cyber Week hosted by Tel Aviv University, Lindy Cameron also discussed how the ties between academia, industry, and governments are key to countering the latest cyber threats.

The CEO of the UK NCSC – which is part of the world-leading intelligence agency GCHQ – will say that even following the illegal Russian invasion of Ukraine, ransomware remains the biggest global cyber threat most organisations must manage.

She will also praised Ukrainian cyber defenders for their response to Russia's invasion, highlighting the resilience of their networks in repelling many attacks. She said:

"Russia has consistently used cyber pressure to stress its rivals, distract them, and where possible disable them.

"But – just as they have on the battlefield – the Ukrainian cyber defenders have done an incredible job of repelling many of these attacks. They are real heroes.

"And I think resilience and preparation are at the heart of this success."

The main focus of her speech was the international regulation of sophisticated cyber capabilities. Lindy Cameron said:

"If we're going to maintain a cyberspace which is a safe and prosperous place for everyone, it is vital that such capabilities are produced and used in a way that is legal, responsible and proportionate.

"I am delighted that Israel has tightened export controls around these tools, making it far more difficult for nations with concerning records on privacy and human rights to acquire such intrusive spyware.

"It is really important that every actor, from the developer to the end-user of these types of technology and capability acts responsibly, with appropriate safeguards to protect against misuse."

Describing Israel as a "shining" example of what can be done when a nation takes cyber security seriously, she said:

"The technology developed here is truly world class. The talent in the cyber security sector is second to none. And your defences are some of the strongest in the world.

"But making the most of our digital future is too big an issue for any one nation to handle alone.

"Whether it is drip feed irrigation or health and climate tech, Israel has always been proud to innovate for the benefit of people, well beyond your borders.

"So, I hope you will continue to produce cyber security solutions which are safe, strong but also affordable for the whole world."

Turning to ransomware and how the upward trend of the commercialisation of such capabilities dramatically lowers the technical knowhow required to conduct criminal operations, she said:

"But - even with a war raging in Ukraine - the biggest global cyber threat we still face is ransomware. That tells you something of the scale of the problem.

"Ransomware attacks strike hard and fast. They are evolving rapidly, they are all-pervasive, they're increasingly offered by gangs as a service, lowering the bar for entry into cyber crime.

"And that's what makes them such a threat – not just the nationally significant incidents that my team and I we deal with in the NCSC, but also the hundreds of incidents we see that affect the UK more widely every year.

"These complex attacks have the potential to affect our societies and economies significantly, if it were not for the expertise of our incident management operators working in collaboration with their counterparts in industry and their international counterparts gathered here today."

Returning to the theme of partnerships, Lindy Cameron emphasised that prosperous relationships between different institutions are key to countering the latest cyber threats:

"To succeed, partnerships are essential. So, we are building stronger ties between academia, industry and government.

"We must come together around our shared values. Each nation bringing its own particular skills and strengths to build a network which is naturally resilient to attack, one which favours innovation, discourse and creativity over control and coercion."

IDF official: Israel thwarted cyberattack targeting US power plants

'It enabled preventing this threat, through tight collaboration with our fantastic American partners'

Israel halted hackers from attacking US power plants, the deputy chief of the Israeli army's signals intelligence branch, Unit 8200, said at Tel Aviv University's annual cyber week on Wednesday.

The IDF official said that his unit became aware of the cyber threat in the process of stopping another attack aimed at Israel.

"We also found that they were attempting to target US power plants as well. This was the first indication of this attack. It enabled preventing this threat, through tight collaboration with our fantastic American partners," Colonel U. told the audience, according to The Jerusalem Post.

He also explained how his unit dealt with the alleged Iranian attack in 2020 targeting Israel's water facilities.

"We saw this attacker attempting to poison the water in an attempt to claim human lives. We mitigated that threat far ahead," he said at the conference.

Cyberattacks have become an increasing threat for states, and Israel is currently facing a cyber war with Iran.

In June, hackers from the Shiite country allegedly targeted Israel's rocket warning system, activating false rocket warning sirens in Israeli cities.

It was revealed just a few days after senior Israeli officials were hacked by Iran to get access to email accounts, stealing confidential information.

The commander also acknowledged the cyber threat Israel is facing, stressing that Unit 8200 is operating in a "quite tough neighborhood."

"Counter cyber operations are a major part of our operations. Once we obtain superiority over the attacker, we then act to deny their capabilities," he said according to The Jerusalem Post.

"First of all, by collaborating with industry and other agencies, but if necessary, we do it on our own, implementing 'our tools' at some point, somewhere along the attack stream. 8200 won't rest until the threat is removed."

"L'Iran est devenu le principal rival d'Israël dans le domaine de la cybersécurité" (chef de la direction nationale de la cybersécurité)

"Quiconque tentera une cyberattaque contre Israël en paiera le prix", a affirmé N. Bennett '

Le Premier ministre sortant Naftali Bennett a averti mardi que quiconque tenterait une cyberattaque contre Israël "en paierait le prix".

"Tout comme il y a la dissuasion nucléaire, il y a la cyberdissuasion. Si quelqu'un nous attaque dans ce domaine, nous riposterons", a déclaré Naftali Bennett, qui s'exprimait à l'occasion de la Cyber Week de l'Université de Tel-Aviv.

Ces commentaires interviennent au lendemain d'une cyberattaque d'envergure ayant paralysé momentanément l'industrie sidérurgique iranienne, survenue quelques jours après le piratage des systèmes d'alerte précoce en Israël, qui a entraîné le déclenchement inopiné des alarmes à Jérusalem et Eilat.

Un groupe anonyme de hackers a revendiqué l'attaque sur les réseaux sociaux, affirmant qu'il avait ciblé les trois plus grandes entreprises sidérurgiques iraniennes en réponse à "l'agression de la République islamique".

Le groupe, se faisant appeler "Gonjeshke Darande", a partagé des images présumées de l'usine de Khuzestan Steel Co., montrant le dysfonctionnement d'une machinerie lourde sur une chaîne de production de barres d'acier qui a provoqué un important incendie.

Des correspondants militaires israéliens généralement bien informés, ont laissé entendre qu'Israël était directement responsable de la cyberattaque de lundi en Iran, menée en représailles au piratage présumé des systèmes d'alerte israéliens.

Lors du même événement de la Cyber Week, Gaby Portnoy, chef de la direction nationale israélienne de la cybersécurité (INCD), a affirmé que l'Iran était devenu le principal rival d'Israël dans le domaine de la cybersécurité avec le Hezbollah et le Hamas.

"Nous les avons à l'œil et nous savons comment ils opèrent", a affirmé Gaby Portnoy.

Le chef de la direction nationale israélienne de la cybersécurité a indiqué qu'Israël était en train de construire un "cyber dôme de fer" destiné à élever le niveau de la cybersécurité, en utilisant de nouveaux mécanismes et des cyberparamètres qui "réduiront les attaques, fourniront de nouvelles mégadonnées, ainsi qu'une approche globale de l'IA pour synchroniser la détection nationale en temps réel".

"Nous sommes en train de passer rapidement de la résilience à la défense proactive, en traquant les cyber-attaquants dans leurs refuges numériques", a souligné Gaby Portnoy, plaidant pour la mise en place de protocoles de cybersécurité pour les infrastructures, l'ensemble du secteur privé et les chaînes d'approvisionnement.

ISRAEL HAYOM
This is where we stand

Gantz: Iran, Hezbollah targeted UNIFIL operations in Lebanon

Hamas' release of video of captive Israeli tantamount to "humanitarian blackmail," defense minister says. Unit 8200 deputy commander says Israel thwarted Iranian plan to poison Israel's water supply.
Lilach Shoval

Defense Minister Benny Gantz on Wednesday revealed Iran and Hezbollah had worked together to attack UN peacekeeping forces in Lebanon.

He called the incident "another blow by Iran and Hezbollah to Lebanese citizens and stability in the country" in an address to the 2022 Cyber Week conference at Tel Aviv University.

Commenting on the footage released by Hamas of Hisham al-Sayed, the Bedouin Israeli held by the terrorist group, the defense minister said the video was an attempt at blackmail through the use of a humanitarian issue: "Hamas is holding the four boys [al-Sayed, Avera Mengistu, and IDF soldiers Hadar Goldin and Oron Shaul, the latter two of whom were killed in fighting in the Gaza Strip in 2014] in violation of international law and ... ethics. Hamas is responsible for this, and our expectation from the international community is to act against this vile conduct by Hamas.

"The State of Israel acts with a variety of means and continues to turn over every stone to bring the boys home. As we've said in the past, this is a humanitarian issue. That's how we see it, and on this basis, we will continue to act. Attempts at blackmail and psychological warfare will not influence our stand and our conduct," he said.

Describing joint activities by Iran and Hezbollah, the defense minister said: "Iran is also operating its emissaries in the realm of cyber. I can reveal today that Iranian security forces, in cooperation with Hezbollah, recently acted to harm the operations of UNIFIL forces in Lebanon. This is through the implementation of a cyber campaign aimed at stealing material on UNIFIL preparedness in the area and its use by Hezbollah. This is another blow by Hezbollah and Iran to Lebanese citizens and Lebanon's stability."

He said, "Israel is familiar with the cyber systems of its rivals and its paths of action. In recent years, we have witnessed a phenomenon of groups of Iranian-backed hackers who act against Israel and other countries. The new emissaries are terrorists with keyboards who will meet the same fate as other terrorist organizations. We know who they are, we strike them and their dispatchers. And today, too, they are in our crosshairs, and not just in the cyber dimension. No attack on Israeli citizens will be ignored. And the responsibility is on the attackers and the state funding and those dispatching them. A cyberattack can be met with a variety of means in the realm of cyber and other areas."

Gantz said: "Iran is leading cyberterrorism and making moves aimed at influencing democratic processes and regimes, as was the case in the US presidential elections and additional attempts Israel is aware of. Actions like those by the Shahid Cawa unit that collected intelligence on ships, gas stations, and industrial factories in a number of countries were carried out under the direct directive of the Iranian leadership and the Revolutionary Guards as was revealed in the investigations."

He noted that in recent years, Israel has prevented "many attempts to hack into private and public firms in Israel and overseas. I also call on the public to demand 'cyber accountability' and punish companies and organizations that do not act in accordance with the guidelines."

Delineating Israel's plans to contend with various threats, Gantz said: "Our chief mission in the military, in the various security industries and organizations, is to build the people, train them, and keep them. The [IDF] Chief of Staff [Lt. Gen. Aviv Kochavi] and I have made this issue one of the central missions of the relevant units. We are constantly examining the buildup of force – in terms of both manpower as well as the issue of training and the issue of missions. In the coming years, we will also need to assess the organization, management, and operation of cyberwarfare, its offensive and defensive traits in the IDF, and the entire security system."

Gantz concluded by calling for cooperation with the world: "There is great importance to our cooperation with the world against Iran and in the realm of cyber. We are expanding this cooperation we are building in the region against Iran in regard to defense and various threats to the cyber realm as well.

In what was his first such public address, Ori, the deputy commander of the IDF's 8200 Intelligence unit, revealed Israel had thwarted an attack on the country's water systems.

"The thwarting of cyber threats is a central part of our activity. Our goal is to achieve superiority over the attacks, to succeed in identifying it, and to act to revoke their abilities. So, sometimes, we also find victims outside of Israel, and then we make contact with other agencies when necessary. We do this both independently and through cooperation with the industry and other agencies through the implementation and use of tools that we have developed. 8200 will not rest until the threat is removed," Ori said.

He said the unit thwarted an attempt to "take over Israel's critical water systems and poison them a few years ago. In another instance, we also identified that a certain enemy had attacked Israel and recognized that the same attacker was also trying to target power stations in the US. This was the first indication of this attack. We succeeded in thwarting this threat through close cooperation with our American partners."

ISRAEL HAYOM
This is where we stand

Suspected cyberattack triggers sirens in Jerusalem, Eilat

The strongest indicator of a hack is the fact that civilian – not military – alert systems were compromised, National Cyber Directorate says. Local authorities instructed "to take preventative measures against the threat."
Ariel Kahana , Yori Yalon and Ronit Zilberstein

The air raid sirens that blared across parts of Jerusalem and the resort city of Eilat Sunday were most likely the result of a cyberattack, the Israel National Cyber Directorate said.

The Cyber Directorate said in a statement that the strongest indicator that the sirens were the result of a hack rather than a malfunction was the fact that the systems that were activated were municipal – not the ones controlled by the IDF's Home Front Command.

"Local authorities have been instructed to take preventative measures against the threat," the statement said.

The INCD said that the source of the attack is unclear at this time, adding that it was investigating whether Iranian hackers were behind the alleged attack.

"It seems that the attack didn't compromise any infrastructure defined as critical, but at the same time, it again became clear how compromising relatively simple civilian systems disrupts Israeli citizens' lives," CEO of Israel Internet Association Yoram Hacohen told Israel Hayom.

He further noted that there is "a significant gap between the excellent protection the state offers what it defines as critical infrastructure and the lacking protection of other civilian infrastructure.

"This isn't the first attack to illustrate this gap. We have to increase awareness and employ better cyber-defenses across the board."

Deputy Economy and Industry Minister Yair Golan touched on the issue in an interview with Army Radio, saying, "There have been many attempts by the Iranians to harm Israel using cyber [measures] and we take it seriously."

Golan, a retired major general who served as deputy chief of staff, added that the fact the civilian warning systems were hacked was "very troubling. If there's a breach it needs to be taken care of immediately."

Omree Wechsler, a senior researcher at the Blavantnik Interdisciplinary Cyber Research Center, said that the hacks targeted public address systems in Jerusalem and Eilat.

"As a clear Israeli symbol, it shows that this is an opportunistic attack and not a sophisticated and well-planned attack launched years ago - the hackers attacked where they found loopholes. As many cyberattacks in the world are focused on financial or espionage targets, the Iranian activity against Israel is in accordance with the pattern of causing damage or creating panic. Such attacks are common and are part of a daily routine that includes thousands of attempts to hack into any system or server whose damage would cause media coverage, in contrast to the espionage activity that also takes place every day," Wechsler said.

Last week, Israeli cybersecurity giant Check Point uncovered an extensive phishing scheme by Iranian hackers seeking to compromise former high-ranking Israeli officials, including former Foreign Minister Tzipi Livni, retired Military Intelligence Amos Yadlin, and a former US ambassador to Israel.

In March, a massive cyberattack downed most Israeli government websites but swift action by the National Cyber Directorate managed to fend it off within minutes.

ISRAEL HAYOM
This is where we stand

State comptroller: Israel not ready for real cyberwar

"Our data is out there and we are exposed. World War III will be dominated by hackers but the world is not ready for it," Matanyahu Englman warns.
Yair Altman

State Comptroller Matanyahu Englman warned last week that Israel is grossly underprepared for the ramifications of an actual cyberwar.

"We are exposed. Our data is visible to too many people. Our transactions are exposed, our children are exposed, our health [information] is exposed, our security is exposed. World War III will be a cyberwar, but the world is not ready for it," Englman said Wednesday at Cyber Week 2022, the annual international cybersecurity expo hosted by Tel Aviv University.

Audits by the State Comptroller's Office have found significant failures in Israel's cyber readiness in major hospitals, Tax Authority, and municipal transportation direction systems, he said.

Many of the public bodies audited were found to have performed only basic hacking drills – some only during the time of the audit he said.

He also warned that the central election committee was unprepared to ward off cyber threats – a point that has significant implications given that Israel is heading toward its fifth elections in three years.

"We at the State Comptroller's Office undertake to continue to address this significant issue, for the benefit of the Israeli public," he concluded.

ISRAEL HAYOM
This is where we stand

PM warns Iran not to 'mess with Israel' as Doha talks begin

Rob Malley, the US special representative for Iran, arrived in Qatar on Monday night ahead of indirect negotiations separate from the official JCPOA nuclear talks in Vienna.
Tamir Morag

Prime Minister Naftali Bennett warned Iran on Tuesday that Israel would not stand idly by if it targets Israel. Speaking at Tel Aviv University's annual international cybersecurity conference Cyber Week Bennett said, "My approach toward our enemies – especially Iran – is that we are not going to create destruction, but those who mess with us will pay a price, and if the thug sends people to hurt us we are going to hit the thug on every dimension." Bennett then added, "If someone attacks us via cyber, we are going to retaliate."

Meanwhile, Iran and the United States appeared poised Tuesday to start indirect talks in Qatar aimed at finding a way to save Tehran's tattered nuclear deal with world powers.

The state-owned Tehran Times posted a photograph of Iran's top nuclear negotiator, Ali Bagheri Kani, in a hotel lobby with Iranian Ambassador to Qatar Hamidreza Dehghani. The newspaper said Bagheri Kani was in Doha, the Qatari capital, for the resumption of the talks.

Rob Malley, the US special representative for Iran, arrived in Qatar on Monday night ahead of the talks. The US Embassy in Qatar said Malley met with Qatari Foreign Minister Mohammed bin Abdulrahman Al Thani to discuss "joint diplomatic efforts to address issues with Iran," but declined to immediately offer any other details about his trip.

Qatar's Foreign Ministry later issued a statement saying it "welcomed" hosting the talks. It said the talks aimed to reestablish the deal "in a way that supports and enhances security, stability and peace in the region and opens new horizons for broader regional cooperation and dialogue with the Islamic Republic of Iran."

Iran and world powers agreed in 2015 to the nuclear deal, which saw Tehran drastically limit its enrichment of uranium in exchange for the lifting of economic sanctions. In 2018, then-President Donald Trump unilaterally withdrew America from the accord, raising tensions across the wider Middle East and sparking a series of attacks and incidents.

Talks in Vienna about reviving the deal have been on a "pause" since March. Since the deal's collapse, Iran has been running advanced centrifuges and rapidly growing stockpile of enriched uranium.

Even as negotiators convened in Doha, Iran's nuclear chief on Tuesday confirmed that Iran had begun installing a new cascade of advanced centrifuges at its underground Fordo facility.

The International Atomic Energy Agency earlier reported that Iran was planning to enrich uranium through a

new chain of 166 advanced IR-6 centrifuges at the site. A cascade is a group of centrifuges working together to more quickly enrich uranium.

"We will follow measures according to the plans made," declared Eslami, without saying at which level the new cascade will be enriching.

Earlier this month, Iran removed 27 surveillance cameras of the IAEA to pressure the West toward making a deal. The IAEA's director-general warned it could deal a "fatal blow" to the accord as Tehran enriches uranium closer than ever to weapons-grade levels.

Nonproliferation experts warn Iran has enriched enough up to 60% purity – a short technical step from weapons-grade levels of 90% – to make one nuclear weapon, should it decide to do so.

Iran insists its program is for peaceful purposes, though UN experts and Western intelligence agencies say Iran had an organized military nuclear program through 2003.

Building a nuclear bomb would still take Iran more time if it pursued a weapon, analysts say, though they warn Tehran's advances make the program more dangerous. Israel has threatened in the past that it would carry out a preemptive strike to stop Iran – and already is suspected in a series of recent killings targeting Iranian officials.

ISRAEL HAYOM
This is where we stand

Bayer to establish cybersecurity hub in Israel

The pharma giant plans to integrate the hub into Bayer's global cyber unit. Local center to be one of the largest internal cyber units the multinational conglomerate operates.

Pharma giant Bayer on Thursday announced plans to establish a cybersecurity hub in Israel, which will be integrated into Bayer's global cyber unit and will be one of the largest internal units of this kind in the company.

A delegation of top Bayer executives arrived in Israel on June 26 for a three-day visit and met with Economy and Industry Ministry Director-General Ron Malka to discuss the German company's plans to deep-dive into the Israeli market.

The planned cybersecurity hub places Bayer Israel in a unique position among locally operating pharma companies, as it will allow it to bring added value to the Israeli business sphere via opportunities to connect to its global operations in health, agriculture, and innovation.

The delegation included, among others, Bijoy Sagar, Bayer's chief information technology and digital transformation officer, and Gary Harbison, head of cybersecurity and risk management, who were the driving force behind the move. The two also spoke at the main plenary of Cyber Week 2022, the annual international cybersecurity expo hosted by Tel Aviv University.

"I am excited by the spirit of innovation, level of talent, and pragmatism I witnessed in the startup ecosystem,

the government, and universities in Israel in the sphere of information technology," Sagar said. "Bayer business in Israel is strong and the cybersecurity bub is another great addition to our initiatives in Israel."

During Cyber Week, top TAU and Bayer executives also inked a cooperation agreement to promote groundbreaking cybersecurity research from Tel Aviv University.

Managing Director of Bayer Israel Hugo Hagen (Courtesy)

"As a company engaged in R&D in the core areas of life sciences, the ability to integrate with Israel's unique cybersecurity ecosystem, alongside sectors such as medical innovation and agricultural development is an opportunity to integrate as players in the Israeli market and provide added value for Bayer and for the ecosystem," Managing Director of Bayer Israel Hugo Hagen said.

"As a Norwegian who has worked in Israel for three years, I feel a mission to promote Israel on Bayer's investment map and to strengthen the company's position within Israel, as well as that of the Israeli headquarters within the global headquarters. The ecosystem here is impressive and it would be a mistake not to try to enjoy the possibilities that exist here, and of course, I am proud that the decision was made to establish the new cyber security unit here."

"There is no doubt that such initiatives contribute to employment, innovation, and Israel's image, and attract other international investments," Malka noted. "We will continue to represent the best Israeli innovation has to offer and link it to leading companies. We welcome Bayer's expansion in Israel and we are working to develop future similar initiatives."

Yael Mor, who will run the hub for Bayer, said, "It is exciting to create something the activities of which will have an impact in the world beyond Israel's borders. Along with our focus on the cyber unit, we will engage in locating Israeli innovation in cyber security."

Bayer is one of the largest pharmaceutical and life sciences conglomerates in the world. Its main areas of business include consumer healthcare products, agricultural chemicals, and seeds and biotechnology products. The company set up its offices in Israel in 2008 and currently employs 150. Worldwide, Bayer maintains a presence in 83 countries, employing some 100,000 people.

ISRAELDEFENSE

Israel is promoting "national Cyber Dome," says cyber chief

INCD head Gabi Portnoy referred to the ongoing cyber war with Iran, saying it has "become out dominant rival"

In his first public speech, Gaby Portnoy, Director General of Israel National Cyber Directorate (INCD), presented the new INCD project aimed to diminish cyber-attacks: The Cyber-Dome - a new big-data, AI, overall approach to proactive defense. Portnoy presented in the annual Cyber Week event led by the INCD and Tel-Aviv University cyber research center.

INCD data presented in the conference revealed that 1,500 attacks were halted during the last year by INCD's teams.

Relating to attackers, Portnoy said: "There is no longer only one-type of an ideological official enemy. On the one hand - Iran has become our dominant rival in cyber, together with, Hezbollah and Hamas. We see them, we know how they work, and we are there. On the other hand, the spectrum also was stretched - to attackers, attack groups, proxies, independent crime-organizations, and private people".

Portnoy presented the INCD's new project: Cyber Dome – an analogy to Israel's Iron-Dome. "The Cyber Dome will elevate national cyber-security by implementing new mechanisms in the national cyber perimeter, reducing the harm from cyber-attacks at scale.

"The Cyber Dome will also provide tools and services to elevate the protection of the national assets as a whole. The Dome is a new big-data, AI, overall approach to proactive-defense. It will synchronize nation-level real-time detection, analysis, and mitigation of threats."

Portnoy added that "We need to protect our national assets in the best possible way and make cybersecurity protocols we use for critical infrastructure available for more sectorial organizations - government and private". He stressed that "You cannot fight cyber aggression alone. You have to have partners, at home, in your defense community, in the government, in the different sectors, in the academy, in the private sector and around the world".

israel heute

Iranische Cyber-Angreifer versuchen, Israel in Panik zu versetzen – bislang ohne Erfolg

Beobachter sagen, der iranisch-israelische Cyberkrieg habe gezeigt, dass die Iraner "opportunistische Schlupflöcher" nutzen – Die Einführung des Quantencomputers könnte neue Möglichkeiten im Cyberbereich eröffnen.

Yaakov Lappin

(JNS) Die iranischen Cyberangreifer, die Israel ins Visier genommen haben, haben sich darauf konzentriert, Panik zu verbreiten, ohne jedoch fortgeschrittene Cyberangriffsfähigkeiten zu aktivieren, sagen Beobachter in Israel und warnen, dass die feindlichen Akteure weiterhin nach neuen Schwachstellen suchen werden.

In diesem Monat haben iranische Cyberangreifer Berichten zufolge die Raketenwarnanlagen der Stadtverwaltungen von Jerusalem und Eilat aktiviert und die E-Mails hochrangiger israelischer und amerikanischer Beamter und Führungskräfte ins Visier genommen.

Im November richtete sich eine Reihe von Cyberangriffen auf iranische Tankstellen und Autobahnschilder im ganzen Land, wobei Berichten zufolge jede Tankstelle im Land lahmgelegt wurde, während gleichzeitig Anzeigen übernommen und subversive regimefeindliche Botschaften angezeigt wurden.

Der israelisch-iranische Cyber-Schattenkrieg scheint also kein Ende zu nehmen. Das 2012 eingerichtete Nationale Cyber-Direktorat Israels (ursprünglich bekannt als Nationales Cyber-Büro) ist eine Regulierungsbehörde, die sicherstellt, dass kritische Webseiten des privaten und öffentlichen Sektors geschützt sind, und die Mindestschutzniveaus festlegt, die für alle kritischen Infrastrukturen und Unternehmen des privaten Sektors erforderlich sind.

„Die Hacks zielten insbesondere auf öffentliche Adressensysteme in Jerusalem und Eilat ab", sagte Omree Wechsler, ein leitender Forscher am Blavatnik Interdisciplinary Cyber Research Center der Universität Tel Aviv. „Als klares israelisches Symbol zeigt es, dass es sich um einen opportunistischen Angriff handelt und nicht um einen ausgeklügelten und gut geplanten Angriff, der vor Jahren gestartet wurde; die Hacker griffen dort an, wo sie Schlupflöcher fanden."

„Da sich viele Cyberangriffe in der Welt auf Finanz- oder Spionageziele konzentrieren, entsprechen die iranischen Aktivitäten gegen Israel dem Muster, Schaden anzurichten oder Panik zu verbreiten. Solche Angriffe sind üblich und Teil einer täglichen Routine, die Tausende von Versuchen umfasst, sich in jedes System oder jeden Server zu hacken, dessen Beschädigung ein Medienecho hervorrufen würde, im Gegensatz zu den Spionageaktivitäten, die ebenfalls jeden Tag stattfinden", erklärte er.

Raum für Verbesserungen in allen Bereichen

Professor Oberst a.D. Gabi Siboni, Experte für Cybersicherheit, militärische Strategie und Technologie am Jerusalemer Institut für Strategie und Sicherheit, erklärte gegenüber JNS, er sei der Meinung, dass „Israel über ein gut funktionierendes System verfügt„ um mit diesen Bedrohungen umzugehen, und das die Bereitschaft aufrechterhält. Natürlich gibt es keine Immunität, und es ist für die Angreifer immer möglich, eine Lücke zu finden und durch sie einzudringen."

Siboni, der als leitender Berater für die israelischen Verteidigungskräfte und andere israelische Sicherheitsorganisationen tätig ist, sagte, es sei wichtig, daran zu denken, dass „nicht nur Regierungssysteme angegriffen werden können, sondern auch zivile Systeme, und dies kann zu erheblichen Schäden führen", bemerkte er und verwies auf den Ransomware-Angriff auf die israelische Versicherungsgesellschaft Shirbit im Jahr 2020, der sich als äußerst schädlich erwies.

„Obwohl das israelische staatliche Verteidigungssystem auch zivile Systeme berührt, ist der zivile Bereich unabhängig und sensibler", sagte er. „Es gibt immer Raum für Verbesserungen in allen Bereichen."

Wechsler sagte, dass es bei der Bewertung der Bereitschaft Israels für diese Art von Angriffen und im weiteren Kontext iranischer Cyberangriffe „wichtig ist, eine Grenze zu ziehen zwischen der Verteidigung militärischer Systeme und Anlagen, kritischer Infrastruktur, deren Bedeutung für den Schutz im Cyberspace Israel als erste Nation erkannt hat, und der Situation im privaten Sektor und den lokalen Gemeinden. Kritische Infrastrukturen, deren Angriffe physische Schäden verursachen können, unterliegen der Leitung des National Cyber Directorate und sind daher gut geschützt."

Er sagte: „Das Gleiche gilt für militärische und nationale Sicherheitssysteme. Diese Angriffe auf die kommunalen Adressensysteme zeigen aber, dass es an Bewusstsein, Regulierung und Durchsetzung mangelt, wenn es um die Cybersicherheit dieser Einrichtungen geht. Das Gleiche gilt für viele private Organisationen, insbesondere für kleine und mittlere Unternehmen, bei denen es keine Behörde gibt, die die Sicherheitsverfahren durchsetzen und überwachen kann."

Auf die Berichte in den internationalen Medien über angebliche israelische Cyber-Offensiven gegen den Iran

angesprochen, sagte Siboni, er versuche, die Gesamtstrategie Israels in dieser Kampagne zu verstehen. „Zwei Seiten tauschen Schläge aus, hin und her, aber was ist die Strategie in diesem Zusammenhang? Diese Frage stelle ich mir immer, und ich kenne die Antwort darauf nicht", räumte er ein.

Wechsler zufolge „gilt Israel in allen Bereichen als hochentwickelter Cyber-Akteur, etwa bei der Cyber-Verteidigung und der Sammlung von Informationen, und verfügt über ein florierendes lokales Cyber-Ökosystem. Wie sich im Laufe der Jahre herausgestellt hat, rangiert Israel auch bei den offensiven Cyberfähigkeiten ganz oben und hat in diesem Bereich weitaus fortgeschrittenere Fähigkeiten als der Iran bewiesen."

„Wir können zwar davon ausgehen, dass diese Fähigkeiten in großem Umfang zum Sammeln von Informationen genutzt werden, aber die Störangriffe von [Berichten über] Stuxnet [Cyberangriff auf iranische Zentrifugenmaschinen] im Jahr 2010 bis hin zu dem Angriff auf den Schahid-Rajai-Hafen in Bander Abbas [Iran] im Mai 2020 zeigen, dass Israel seine Fähigkeiten angeblich nutzt, um den iranischen Nuklearplan zu stören und zu beeinträchtigen, den Israel als existenzielle Bedrohung ansieht", so Wechsler. „Wir können die Sabotage anderer [iranischer] Pläne, wie ballistische Raketen und fortschrittliche Drohnen, und [israelische] Vergeltungsmaßnahmen gegen Angriffe auf seine eigene kritische Infrastruktur nicht ausschließen."

Mit Blick auf die Zukunft sind sich Siboni und Weschler einig, dass das Quantencomputing einen Durchbruch bei den Fähigkeiten zur Cyber-Kriegsführung darstellen wird.

„Die Fähigkeiten entwickeln sich ständig weiter, sowohl bei Angreifern als auch bei Verteidigern", sagte Siboni. „Ich sehe keinen großen Durchbruch, solange wir nicht in den exotischen Bereich der Quanteninformatik vordringen, was wahrscheinlich in absehbarer Zeit geschehen wird. Bis dahin wird sich jede Seite schrittweise verbessern, Schwachstellen finden und darauf reagieren.

Wechsler sagte, dass „die Fortschritte bei den Cyber-Bedrohungen und -Fähigkeiten in zwei Richtungen verlaufen".

„Einerseits", erklärte er, „ist es kein Geheimnis, dass die Staaten viele Ressourcen investieren, um fortschrittlichere Fähigkeiten zu entwickeln, die sie zur Nachrichtengewinnung und als Teil des militärischen Instrumentariums einsetzen. Andererseits sind wir umso anfälliger für diese Bedrohungen, je digitaler und vernetzter wir werden. Trends wie ‚alles vernetzen' und das Internet der Dinge (IoT) vergrößern die Angriffsfläche, während aufkommende oder künftige Technologien wie künstliche Intelligenz und Quantencomputer sowohl die Verteidigungs- als auch die Angriffsfähigkeiten durch mehr Rechenleistung und Automatisierung verbessern dürften.

Dieselben Technologien könnten jedoch auch die Sicherheit erhöhen, schätzte er ein, und fügte hinzu, dass „wir mit den richtigen Vorschriften, Grundsätzen und Normen auch viele der Risiken abmildern könnten."

Noticias de Israel

Ciberataques de Irán intentan sin éxito sembrar el pánico en Israel

"Dado que muchos ciberataques en el mundo se centran en objetivos financieros o de espionaje, la actividad iraní contra Israel se ajusta al patrón de causar daños o crear pánico.

Los ciberatacantes iraníes contra Israel se han centrado en intentar sembrar el pánico; sin embargo, no han activado capacidades avanzadas de ciberataque, dicen los observadores en Israel, al tiempo que advierten que los actores hostiles seguirán buscando nuevas vulnerabilidades.

Este mes, los ciberatacantes iraníes habrían activado las sirenas de cohetes de las autoridades municipales de Jerusalén y Eilat, además de atacar los correos electrónicos de altos funcionarios y ejecutivos israelíes y estadounidenses.

En noviembre, una serie de ciberataques tuvieron como objetivo gasolineras y señales de carretera iraníes en todo el país, al parecer inutilizando todas las gasolineras del país, al tiempo que secuestraban pantallas y proyectaban mensajes subversivos contra el régimen iraní.

De este modo, parece que la ciberguerra en la sombra entre Israel e Irán no tiene un final a la vista. La Dirección Cibernética Nacional de Israel, creada en 2012 (originalmente conocida como Oficina Cibernética Nacional), es un regulador que garantiza la protección de los sitios web críticos del sector público y privado, y define los niveles mínimos de protección necesarios para todas las infraestructuras críticas y empresas del sector privado.

"En concreto, los hackeos se dirigieron a los sistemas de dirección pública de Jerusalén y Eilat", dijo Omree Wechsler, investigador principal del Centro Interdisciplinario de Investigación Cibernética Blavatnik, de la Universidad de Tel Aviv. "Como claro símbolo israelí, demuestra que se trata de un ataque oportunista, y no de un ataque sofisticado y bien planificado lanzado hace años; los hackers atacaron donde encontraron resquicios".

"Dado que muchos ciberataques en el mundo se centran en objetivos financieros o de espionaje, la actividad iraní contra Israel se ajusta al patrón de causar daños o crear pánico. Este tipo de ataques son comunes y forman parte de una rutina diaria que incluye miles de intentos de hackear cualquier sistema o servidor cuyo daño pueda causar cobertura mediática, en contraste con la actividad de espionaje que también tiene lugar cada día", afirmó.

"Espacio para mejorar en todos los ámbitos".

El profesor coronel (res.) Gabi Siboni, experto en ciberseguridad, estrategia militar y tecnología en el Instituto de Estrategia y Seguridad de Jerusalén, dijo a JNS que evalúa que "Israel tiene un sistema bien engrasado para hacer frente a estas amenazas y que mantiene la preparación. Por supuesto, no hay inmunidad, y siempre es posible que los atacantes localicen una brecha y entren por ella".

Siboni, que trabaja como asesor principal de las Fuerzas de Defensa de Israel y de otras organizaciones de seguridad

israelíes, dijo que era importante recordar que "no sólo los sistemas gubernamentales pueden ser atacados: los sistemas civiles pueden verse perjudicados, y se pueden causar daños significativos", señaló, refiriéndose al ataque de ransomware de 2020 a la compañía de seguros israelí Shirbit, que resultó muy perjudicial.

"Aunque el sistema de defensa del Estado israelí también toca los sistemas civiles, la esfera civil es independiente y más sensible", dijo. "Siempre hay margen de mejora en todas las esferas".

Wechsler dijo que al evaluar la preparación de Israel para este tipo de ataques y en el contexto más amplio de los ciberataques iraníes, "es importante trazar una línea entre las defensas aplicadas a los sistemas e instalaciones militares; las infraestructuras críticas, de las que Israel fue la primera nación en reconocer la importancia de proteger en el ciberespacio; y la situación en el sector privado y los municipios locales". Las infraestructuras críticas, cuyo ataque puede causar daños físicos, están sujetas a la dirección de la Dirección Cibernética Nacional y, por tanto, están bien protegidas".

Dijo que "lo mismo ocurre con los sistemas militares y de seguridad nacional. Estos ataques a los sistemas de la dirección municipal indican una laguna en la concienciación, la regulación y la aplicación de la ley en lo que respecta a la ciberseguridad de estas entidades. Lo mismo ocurre con muchas organizaciones privadas, especialmente las pequeñas y medianas empresas, donde no hay ningún organismo que pueda hacer cumplir y supervisar los procedimientos de seguridad".

Cuando se le pidió que comentara las informaciones aparecidas en los medios de comunicación internacionales sobre supuestas operaciones israelíes de ciberofensiva contra Irán, Siboni dijo que está tratando de entender la estrategia general de Israel en esta campaña. "Las dos partes intercambian golpes, de ida y vuelta, pero ¿cuál es la estrategia en este contexto? Siempre esta pregunta, y aquí no sé cuál es la respuesta", reconoció.

Según Wechsler, "se considera que Israel es un actor cibernético sofisticado en todos los ámbitos, como la ciberdefensa y la recopilación de información, y que tiene un floreciente ecosistema cibernético local". Por lo que se ha revelado a lo largo de los años, Israel también ocupa un lugar muy alto en las capacidades cibernéticas ofensivas y ha demostrado tener capacidades mucho más avanzadas que Irán en ese campo".

"Aunque ciertamente podemos suponer un amplio uso de estas capacidades para la recopilación de inteligencia, los ataques de interrupción desde [los informes sobre el] Stuxnet [ciberataque a las máquinas centrífugas iraníes] en 2010 hasta el ataque que tuvo como objetivo el puerto de Shahid Rajai en Bander Abbas [Irán] en mayo de 2020 muestran que Israel supuestamente utiliza sus capacidades para interrumpir y degradar el plan nuclear de Irán, que Israel ve como una amenaza existencial", dijo Wechsler. "No podemos descartar el sabotaje de otros planes [iraníes], como los misiles balísticos y los drones avanzados, y las represalias [israelíes] contra los ataques que tienen como objetivo sus propias infraestructuras críticas".

De cara al futuro, tanto Siboni como Weschler coincidieron en que la computación cuántica representaría un gran avance en las capacidades de ciberguerra.

"Las capacidades siempre se están desarrollando, tanto para los atacantes como para los defensores", dijo Siboni. "No veo un avance importante a menos que entremos en el área exótica de la computación cuántica, lo que probablemente ocurrirá en un futuro previsible. Hasta entonces, cada parte mejorará gradualmente, encontrando puntos débiles y actuando sobre ellos".

Wechsler dijo que "los avances en las amenazas y capacidades cibernéticas son bidireccionales".

"Por un lado", explicó, "no es ningún secreto que los Estados invierten muchos recursos para desarrollar capacidades más avanzadas que aplicar para la recopilación de información y como parte de la caja de herramientas de sus ejércitos. Por otro lado, cuanto más digitales y conectados estamos, más susceptibles somos a estas amenazas. Tendencias como "conectarlo todo" y el Internet de las cosas (IoT) amplían la superficie de ataque, mientras que se espera que las tecnologías emergentes o futuras, como la inteligencia artificial y la computación cuántica, aumenten las capacidades defensivas y ofensivas al añadir más potencia de cálculo y automatización".

Sin embargo, las mismas tecnologías podrían, según él, impulsar también la seguridad, añadiendo que "con los reglamentos, principios y normas adecuados, también podríamos mitigar muchos de los riesgos".

israel today.

ANALYSIS: Israel Further Escalates Covert War Against Iran as Nuclear Talks Resume

Disgruntled Iranian commanders admit Israel is getting the better of them, as the Jewish state's cyber superiority takes center stage.
Yochanan Visser

Talks over a new or amended nuclear deal between Iran and some world powers resumed on Tuesday in Qatar, the only Arab Gulf state with which Iran has good relations.

This was very much against the wishes of Israel, and outgoing Foreign Minister Yair Lapid expressed disapproval of these renewed negotiations that will take place despite increasing aggression by Iran in its conflict with Israel.

The resumption of indirect talks between a team of US negotiators and representatives of the radical regime in Tehran had been encouraged by the European Union.

Joseph Borrell, the EU diplomat responsible for the organization's foreign policy, was in Tehran last week and wrote on Twitter that it was necessary to break the current "dynamics of escalation."

Iran, however, remained coy about the 'breakthrough' and told the US to remain "realistic," meaning all sanctions against the Islamic Republic must be lifted.

The US government of President Joe Biden responded to news that Borrell had managed to break the deadlock by making another concession to Tehran.

Media in the US and Israel reported that some members of the Islamic Revolutionary Guard Corps would now be re-allowed to enter the United States.

Lapid lashes out

Lapid, who this week will take over as Israel's interim prime minister, condemned Borrell's visit to Iran.

Lapid said Borrell's position was "very disappointing" in light of the latest Iranian sabotage activity in the monitoring of the Islamic Republic's nuclear facilities by the International Atomic Energy Agency (IAEA).

Iran recently removed IAEA cameras from a number of its nuclear facilities, and this led to strong condemnations from most members of the IAEA and the adoption of a resolution by the agency's governors censuring the Islamic Republic.

The removal of the IAEA monitoring cameras rendered the inspection of Iran's nuclear activities useless, said Rafael Grossi, the Director-General of the UN nuclear watchdog.

See: Iran Will Go Nuclear, Laments IAEA Chief

Lapid personally told Borrell that his actions were a "strategic mistake that sent the wrong signal" to Iran.

The top Israeli diplomat accused his EU counterpart of a "worrying lack of concern for the lives of Israeli citizens."

See: Our Lukewarm and Fearful Responses to Iran Are Not Biblical

This was a reference not only to Iran's nuclear threat but also to the events in Turkey, where members of Iran's Islamic Revolutionary Guard Corps (IRGC) hunted down Israeli civilians last week.

What to do about Iran?

In Israel, top military and intelligence officials are divided over the usefulness of resuming nuclear negotiations with Iran in Qatar.

For example, Aviv Kochavi, the Chief of Staff of the Israel Defense Forces (IDF), opposes the renewed negotiations with Iran.

The same goes for David Barnea, the current head of Mossad, Israel's foreign secret service.

Both Kochavi and Barnea believe that the only way to stop Iran from advancing its nuclear program and curb its imperialist actions in the Middle East is for Israel to use its military and intelligence superiority.

Others think, however, that a new nuclear deal could still keep Iran from breaking out to an atomic bomb.

The EU team in Qatar on Thursday morning announced that two days of indirect negotiations had failed to bring the anticipated breakthrough.

Iran reportedly stuck to old positions and even demanded new things not related to the nuclear dossier.

This shows again that the Israeli intelligence and military chiefs were right about Iran's stalling tactics and the need to use covert warfare tactics to halt Iran's nuclear and imperialistic drive.

Shadow war

Under Barnea, Mossad has recently stepped up its activities against Iran, especially within the borders of the Islamic Republic, and infiltrated the IRGC, a disgruntled top member of the organization admitted this week.

The New York Times reported on Wednesday that Hossein Ta'ab the head of the IRGC's intelligence division, who was removed from his position last week, had told the paper that Israel's actions inside Iran had "undermined our most powerful intelligence organization."

Ta'ab's admission finally confirmed that the Israeli intelligence organizations are aware of most of Iran's terrorist plots against targets within and outside the Jewish state.

Ta'ab's removal from one of Iran's top jobs came after the secret arrest of another IRGC general, Ali Nasari, who also served in the IRGC's intelligence service and was reportedly spying for Mossad.

Cyber superiority

On Monday, General Kochavi visited IDF Unit 8200, which is also known as SIGINT.

SIGINT is a special intelligence unit of the Israeli army that is responsible for most cyber attacks on targets in Iran.

These cyber-attacks are increasingly part of the so-called 'covert war' between Iran and Israel, which has escalated significantly in recent months.

This escalation was the result of a political decision by outgoing Prime Minister Naftali Bennett, who in January said that Israel should take the fight against Iran to the "head of the octopus."

Since then, not a week has gone by in Iran without sabotage acts, assassinations, or cyber attacks that were mostly attributed to Mossad or the SIGINT unit.

The latest cyber attack on vital installations in Iran took place last Monday, when three major factories producing steel were sabotaged.

As a result of these cyber attacks, Iran's entire steel production came to a standstill, which in turn had serious consequences for the large military industry of the Islamic Republic.

The attacks were carried out by a group of hackers called 'Predatory Sparrow,' a group that was previously responsible for cyber attacks that paralyzed fuel supply and rail transport in Iran.

The group must have the backing of "a state-actor," Israeli cyber experts say.

Without precise intelligence about the three steel factories and the physical presence of collaborators, these cyber attacks could not have caused the damage that almost destroyed the facilities.

Military commentators later stated that Israel was definitely behind the new cyber attacks on Iran.

The group of hackers was previously associated with the Israeli security apparatus, specifically the IDF's SIGINT unit.

After the attack, the group of hackers released a statement on social media saying it was a response to "the aggression of the Islamic Republic."

Iranian hackers thwarted

The new cyber attack on Iran's metal industry came more than a week after sirens suddenly went off in the Israeli cities of Eilat and Jerusalem.

The IDF's Home Front division later announced that the sirens were false alarms caused by a cyber attack from a group of hackers in Iran.

SIGINT's deputy commander 'Uri' also made a rare appearance at the Cyber Conference of Tel Aviv University, where he explained how his unit prevented a group of Iranian hackers from poisoning Israel's fresh water supply.

SIGINT was aware of the planned hack long before the attack was carried out and managed to neutralize it before scores of Israelis would have been killed, 'Uri' said.

Due to the military censor, the full name of the SIGINT commander was barred from publication.

Israel's National Cyber Directorate has now launched a new project called "Digital Iron Dome" to protect companies and other civilian projects from cyber attacks.

The name Iron Dome was taken from the successful anti-missile shield of the IDF.

Don't mess with Israel

Bennett addressed the Iranian cyber threat to Israel during a speech at a week-long Cyber Conference in Tel Aviv.

"We are not causing havoc on the streets of Tehran, that has never been our policy. Our policy is that if you mess with Israel, you will pay a price," Bennett said.

He added that just as there is a nuclear deterrent, there is also deterrence in the Cybersphere.

It was clear that Bennett also disagrees with Borrell's position that negotiations with Iran will "break the dynamics of escalation."

Bennett will continue to be in charge of overseeing the covert war against Iran after handing over the task of Prime Minister to Yair Lapid, who is not an expert on military issues.

MEMO MIDDLE EAST MONITOR

Iran is dominant rival to Israel in cyberwarfare, Israel cyber chief admits

Israel's cybersecurity chief has admitted that Iran – along with the militant groups, Hezbollah and Hamas – is its most dominant rival in regards to cyberwarfare, as the cyberwar between Tehran and Tel Aviv continues to escalate.

The Israel National Cyber Directorate (INCD) head, Gaby Portnoy, made the comments at Tel Aviv University's Cyber Week today, saying that "We see them, we know how they work and we are there."

Portnoy confirmed that Israel is constructing a "cyber iron dome" which will use new mechanisms and technology to strengthen the country's cybersecurity sphere, "reduce cyberattacks, provide new big data and an AI [artificial intelligence] overall approach to synchronise nationwide real-time detection".

He stressed that "we are moving faster from resilience to proactive defence" by targeting attackers in their online and digital safe havens. The INCD head also expressed the need for the application of "cybersecurity protocols for infrastructure" for the wider public, which would involve providing tools and skills to the Israeli private sector and supply chains.

Portnoy's acknowledgment of Iran being Israel's dominant cyber rival comes a day after a cyberattack hit the major Iranian steel firm, Khuzestan Steel Company and its facilities yesterday, forcing it to halt production.

Although the attack was not directly carried out by Israel and was, instead, conducted by an Iranian opposition hacker group, it came a week after false siren alert went off in the cities of Jerusalem and Eilat, which Tel Aviv suspects was caused by an Iranian cyberattack.

MEMO MIDDLE EAST MONITOR

Israel's Bennett says cyber tech could replace commandos

Israeli Prime Minister Naftali Bennett said yesterday that Israeli IT specialists on their keyboards could replace sending commandos to fight in battlefields.

Speaking at the Tel Aviv University Cyber Week, Bennett said: "Just like there is nuclear deterrence, there is going to be cyber deterrence."

He added: "My approach generally, and especially with Iran is that we do not go around wreaking havoc in Tehran, that has never been our policy, but our policy is if you mess with Israel, you will pay a price."

The outgoing Israeli prime minister also said: "You can no longer hit Israel indirectly and through proxies and think you'll get away with it."

"If you are a bully who sends folks – we will try to hit you... Anyone attacking us in cyber, we are going to attack back. We are not going to be feeble here."

"We can get stuff done hitting your enemy through cyber. Before we needed to send 50-100 commandos behind enemy lines with huge risks."

"Now, we get a bunch of smart folks together sitting at a keyboard and achieve the same effect...It is inevitable that cyber is going to become one, if not the most, prominent dimension of future warfare."

MANILA BULLETIN

CyberWeek: A grand showcase of Israel's cybersecurity supremacy

The international media, invited by the Israeli government to join the 12th annual cyberweek. CyberWeek, held jointly by the Blavatnik Interdisciplinary Cyber Research Center (ICRC), The Yuval Ne'eman Workshop for Science, Technology and Security, Tel Aviv University, the Israeli National Cyber Directorate under the Prime Minister's Office, and the Ministry of Foreign Affairs is a leading international conference in cybersecurity.

His Excellency the Hon. Ilan Fluss, Ambassador of Israel to the Philippines invited the Manila Bulletin Technews to participate in this year's Cyberweek, an annual international cybersecurity event hosted at Tel Aviv University in Israel. Over the past 12 years, Cyber Week has become internationally acclaimed as one of the top cybersecurity events in the world.

Cyberweek is where cybersecurity experts, industry leaders, startups, investors, academics, diplomats, and government officials openly share knowledge, methods, and ideas on how to stay safe from cybercriminals and nation-state attacks. A nation-state attack is a serious and growing threat faced by organizations of all sizes. Attackers' primary objective is to gain a strategic advantage for their country by stealing secrets, gathering cyber intelligence, and conducting surveillance against another country.

Israel's initiative to gather all who matter in cybersecurity in one place is an extraordinary achievement. With more than a hundred different events, seminars, and meetings, and a limited time to cover everything, Ran Natanzon, the Head of Innovation and Brand Management of the Foreign Ministry of Israel, with Adva Weiss expertly arranged the schedule of the select group of international media to understand Israel's complicated cybersecurity industry

Cybercrime dramatically increased during the pandemic. Online scams spiked by more than 400% in 2020 compared to previous years. Phishing emails grew significantly that Google blocked over 18 million malware and phishing emails related to COVID-19 daily. This includes spear-phishing for espionage purposes. A recent study titled "The impact of COVID-19 on cybercrime and state-sponsored cyber activities" by Johannes Wigg found out that groups of hackers believed to be sponsored by Russia, China, and North Korea used personalized emails containing references to the pandemic to infect their targets with malware or steal passwords. And according to the US Healthcare Cybersecurity Market 2022 report, more than 90% of healthcare organizations suffered at least one cybersecurity breach. With all these and the previous threats throughout the years, plus the recent cyber attacks targeting civilians, there is a need for a place to talk about and face these threats head-on.

Cyberweek highlights the need for everyone to take cybersecurity seriously as cybercriminals not only target government agencies and private institutions. Senior citizens, ordinary employees, and even kids are now targeted as they are the most vulnerable sector of society.

Cyberweek also reminds the governments that to take down state-sponsored attackers, they need to cooperate and work together. Gaby Protnoy, Director General of Israel National Cyber Directorate, said, "To stop hackers and protect every citizen, we need everyone's cooperation. We need to collaborate to win against online threats." Portnoy added, "you cannot fight cyber aggression alone, and you have to have partners. At home, in your defense community, the government, the different sectors, the academy, the private sector, and worldwide." At Cyberweek, Cyber Emergency Response Team – Israel (CERT-IL) also emphasized the need to spend to protect networks and systems. CERT-IL handles cyber incidents in the civilian sphere in Israel. "You need to have a budget for advanced tools and invest in people to use these tools efficiently," Erez Tidhar, Executive Director of CERT-IL told the media at the CERT-IL headquarters in Beer Sheva, Israel. "Every dollar you spend on cybersecurity, you save 80 dollars when sophisticated hackers target you," he added.

The 12th Cyberweek in Tel Aviv shows that governments are willing to share and cooperate to contain cyber attacks from nation-state attackers and cyber criminals victimizing ordinary netizens. Israel also presented to the world its superiority when it comes to cybersecurity, an accomplishment many countries are trying to emulate. The Philippines, for example, sent delegations from the Technical Education and Skills Development Authority (TESDA) and the Philippine National Police (PNP) to learn how Israel successfully integrated cybersecurity into the people's lives. (I will publish the out-of-this-world cybersecurity research and innovation Israel is doing in a separate story.) Most importantly, Cyberweek brought together ethical cybersecurity enthusiasts and decision-makers to discuss how to effectively fight cyber criminals and nation-state attackers on the Internet without breaking any law.

MANILA BULLETIN

12th Annual Cyber Week kicks off in Israel

Cyber Week is an annual international cybersecurity event hosted at Tel Aviv University in Israel. Over the past 12 years, Cyber Week has become internationally acclaimed as one of the top cybersecurity events in the world.

With more than 9,000 attendees from more than 80 countries, Cyber Week is a place where cybersecurity experts, industry leaders, startups, investors, academics, diplomats, and government officials share knowledge, methods, and ideas on how companies and individuals stay safe from cybercriminals and internet bad actors.

Governments and businesses have prioritized cybersecurity, especially during the pandemic, where cybercriminals have increased and improved their tactics to breach organizations because of the hybrid work and online learning setups.

Cybercrime dramatically increased during the pandemic. 1) Online scams spiked by more than 400% in 2020 compared to previous years. 2) Phishing emails grew significantly that Google blocked over 18 million malware and phishing emails related to COVID-19 daily. This includes spear-phishing for espionage purposes. 3) A recent study titled "The impact of COVID-19 on cybercrime and state-sponsored cyber activities" by Johannes Wigg found out that groups of hackers believed to be sponsored by Russia, China, and North Korea used personalized emails containing references to the pandemic to infect their targets with malware or steal passwords. And 4) More than 90% of healthcare organizations suffered at least on cybersecurity breach, according to the US Healthcare Cybersecurity Market 2022 report.

Cyber Week 2022 will not only help face these issues head-on, but it will also try to assist governments and organizations in confronting cyber threats by introducing the latest technologies and techniques in fighting cybercriminals.

Cyber Week is held jointly by the Blavatnik Interdisciplinary Cyber Research Center (ICRC), The Yuval Ne'eman Workshop for Science, Technology and Security, Tel Aviv University, the Israeli National Cyber Directorate under the Prime Minister's Office, and the Ministry of Foreign Affairs is a leading international conference in cybersecurity.

Manila Bulletin Technews will be here in Israel to bring you the latest in cybersecurity during the duration of the Cyber Week 2022.

MANILA BULLETIN

TESDA, to offer national certification for cybersecurity

(Following the steps of the Israeli government to secure its country against cyber attacks, the Technical Skills, and Education Authority (TESDA) of the Philippines is planning to offer a national certification (NC) for cybersecurity. TESDA Executive Director for Information and Communications Technology Jeffry Ian Dy was recently invited to the 12th Cyberweek to learn how the Israeli government successfully integrated cybersecurity into the schools' curricula. TESDA, through Dy's recommendation, seeks the assistance of Israel to develop the Philippines' national certification for cybersecurity. Below are his learnings and reflections on the recently concluded Cyberweek — Art Samaniego, editor)

The Deputy Commander of Unit 8200 of the Israel Defense Force (IDF) gave his keynote address at the 12th annual Cyberweek here in Tel Aviv, Israel. Unit 8200 is an Israeli Signals Intelligence Corps created to defend Israel's information assets from online attacks. The unit is also responsible for collecting signal intelligence (SIGINT) and code decryption.

Introduced only as "Colonel Yuri," he repeatedly reminded the audience that it is not his real name. He talked about his experience with an ongoing silent war on the internet. He gave more pragmatic and practical information on the same picture presented by the incumbent and former Directors of National Cyber Directorates and National Security Advisors of major NATO powers who spoke before him. His presentation was full of examples of national government sites and critical infrastructures being attacked, not only by nation-states but by cybercriminals who were encouraged by the relatively profitable and easy-to-enter field of cybercrime. His message was that in the last two years, cybercriminals not only target individuals or corporations, but they now target national databases. These cybercriminals use triple extortion schemes, first, where they ask for ransom money to reveal the system's weaknesses. Second, get ransom money for not disclosing that the system was compromised to the public, and third, get a ransom not to leak citizens' personal information to other cybercriminals. Also, cybercriminals can endanger lives as ransomware attacks can cause massive power failures, hospital information systems to go down, and national citizens' databases to be compromised.

Col. Yuri's keynote lasted only 15 minutes. Still, it was enough to terrify me so much that I started reflecting on whether or not my country, the Philippines, is prepared to defend our information assets in cyberspace.

Note that 80% of the war against cybercriminals is waged silently. This war is made by professionals on both sides behind computers and keyboards. In most cases, the public is only informed by cybercriminals themselves as part of their triple extortion modus to frighten the public and pressure governments to concede to their demands. Take the example of Costa Rica when in 2021, President Rodrigo Chavez declared a National Emergency as cyber crooks from a hacking hive named "Conti" held hostage through ransomware, the country's public hospital system. The same modus operandi also happened recently in the Philippines. During the last election, a group called "XSOX" (who are amateurs compared to Conti as the latter now has a US $10M bounty from the US State Department) tried to extort money from Philippine Election provider Smartmatic. When the company refused, XSOX leaked Smartmatic employee information, which in some included full names and mobile numbers, to the public. This led to a Senate investigation. While XSOX revealed some relevant election information, the senate investigation made it clear that the election was not compromised as a result of the hack. While the security breach could not change the outcome of the polls, Comelec and Smartmatic officials who denied that no breach ever took place were publicly humiliated.

Then there is the problem of attribution. As a cyberwar rage on the internet, it is always difficult to pinpoint who is responsible for the crime. Is the country equipped with the proper tools and personnel to identify the perpetrators accurately? Going back to our example on XSOX, they are now out on bail because the evidence is weak. I am confident the PNPs Cybercrime group will reveal more evidence, but it is what it is right now. In most cases, the perpetrators can only be determined by counter-hacking. This is a practice where law enforcement agencies also hack the other group in an effort to plant a "tracker" in the cybercriminals' computers which helps law enforcement find the criminals and also makes digital forensics easier.

But the most critical aspect of cybersecurity is human capital. Does the Philippines have enough human resources trained in cybersecurity to defend our information assets? Manila Bulletin published an interesting article in December 2021. The article's central thesis is that in a survey of industries, it was clear we lack cybersecurity professionals in the country. Consider that higher learning courses in Information Security was only introduced in the country within the last five years. These schools, including my alma mater, the University of the Philippines, lack suitable cyber ranges and laboratories to give students hands-on experience in blue and red team cyber operations. Most of our country's cybersecurity professionals were certified by private vendors. But the outlook is improving. The Technical Skills and Education Authority (TESDA) is trying to build a vendor-neutral national certification for cybersecurity. As per TESDA's competency-based qualifications framework, the qualification will be designed with the assistance of the private sector, companies engaged in cybersecurity, the academe, and government offices primarily engaged in cybersecurity (e.g., the Department of Information and Communications Technology). This is the reason why TESDA officials were invited by the Israel Ambassador to the Philippines, HE Ilan Fluss to attend Cyberweek. TESDA reached out to the Israel government, arguably the cybersecurity capital of the world, to assist in developing the country's national certification for cybersecurity.

This brings us to my last point: Cybersecurity needs a multidisciplinary approach that ties up not only technical personnel but also psychologists, sociologists, political scientists, and lawyers, among others. This is not a job for the government only. Our defenses are only as good as the weakest link. So perhaps the approach to cybersecurity should be changed from assigning the task to a central government agency but by creating a council where the academe and the private sectors in each industry can contribute. The council can share ideas and even share tools. The national cyber range purchased by the DICT can be shared with council members to enhance the country's disaster preparedness in case of cyber-attacks. The information must be shared across all units.

This is the only way to fight this war. By giving cybercriminals a message: "If you mess with one of us, you mess with all of us."

ไทยรัฐ TV

เปิดโลก “ภัยไซเบอร์” ที่อิสราเอล

ปฏิเสธไม่ได้ว่าคอมพิวเตอร์ ระบบอินเตอร์เน็ต สื่อดิจิทัล และเครือข่ายทางสังคมออนไลน์มีบทบาทสำคัญต่อการใช้ชีวิตในทุกวงการ ไม่ว่าจะเป็นเรื่องส่วนตัวทั่วไป อย่างการสื่อสาร การจับจ่ายใช้สอย ทำธุรกรรมทางการเงิน การเก็บข้อมูลส่วนบุคคลจำนวนมากขององค์กร ไปจนถึงการควบคุมการใช้งานอุปกรณ์อิเล็กทรอนิกส์ต่างๆผ่านทางเครือข่ายอินเตอร์เน็ต และการระบาดใหญ่ของโควิด-19 ที่เป็นความท้าทายครั้งใหญ่ของมนุษยชาติส่งผลกระทบอย่างรุนแรงต่อผู้คนทั่วโลก ทั้งการใช้ชีวิตและวิธีการทำงาน กระตุ้นการใช้เทคโนโลยีดิจิทัลอย่างก้าวกระโดด

และเมื่อมีการใช้อินเตอร์เน็ตก็ย่อมเป็นการเปิดช่องให้ถูกโจมตีทางไซเบอร์ได้ทุกขณะและทุกรูปแบบ ซึ่งอาชญากรไซเบอร์ไม่ได้มุ่งเป้าเฉพาะตัวบุคคลเท่านั้น แต่ยังหมายตาระบบโครงสร้างพื้นฐานของภาครัฐรวมถึงธุรกิจขององค์กรโดยมีเงินเป็นแรงจูงใจ “ความมั่นคงปลอดภัยไซเบอร์” จึงไม่ใช่เรื่องไกลตัวแต่เป็นประเด็นที่ทุกฝ่ายต้องให้ความสำคัญ

ในการประชุมระดับนานาชาติด้าน “ความมั่นคงปลอดภัยในโลกไซเบอร์” หรือ “Cyber Week” งานใหญ่ประจำปีที่ได้รับการยกย่องว่าเป็น “อีเวนต์” สำคัญที่ได้รับการยอมรับมากที่สุดในโลก ภายใต้ความร่วมมือของศูนย์วิจัยไซเบอร์บลาวาตนิกเซ็นเตอร์ (ICRC), ศูนย์ประชุมเชิงปฏิบัติการด้านวิทยาศาสตร์ เทคโนโลยี และความปลอดภัย ยูวาล เนมัน มหาวิทยาลัยเทลอาวีฟ, สำนักงานไซเบอร์แห่งชาติอิสราเอล (Israel National Cyber Directorate) ภายใต้สำนักนายกรัฐมนตรีและกระทรวงการต่างประเทศอิสราเอลร่วมเป็นเจ้าภาพจัดงานในระหว่างวันที่ 27-30 มิ.ย. ที่มหาวิทยาลัยเทลอาวีฟ ในนครเทลอาวีฟ เมืองใหญ่อันดับ 2 ของอิสราเอล หรือที่หลายคนเรียกว่า “ซิลิคอน วัลเลย์แห่งตะวันออกกลาง” ศูนย์กลางเทคโนโลยีที่ร้อนแรงและล้ำหน้าที่สุดแห่งหนึ่งของโลก
ภายในงานเปิดโอกาสให้ผู้เชี่ยวชาญจากภาคอุตสาหกรรม หน่วยงานราชการ ทหารนักวิชาการ สถาบันการศึกษา รวมถึงสตาร์ตอัพ นักลงทุน รวมถึงนักการทูต ทุกเพศ-วัย มากกว่า 9,000 คน จาก 80 ประเทศ มานำเสนอนวัตกรรมแลกเปลี่ยนความรู้และเทคโนโลยี แบ่งปันประสบการณ์และความท้าทายจากภาวะกลืนไม่เข้าคายไม่ออกจาก “ภัยคุกคามทางไซเบอร์” ที่นับวันยิ่งซับซ้อนและรุนแรง รวมถึงเปิดเวทีสนทนาในประเด็นหลากหลายเพื่อกระตุ้นแนวคิดใหม่ๆ ในบรรยากาศสุดคึกคักกระฉับกระเฉงมีพลัง และที่สำคัญทีมข่าวต่างประเทศ นสพ. ไทยรัฐยังได้รับโอกาสพิเศษจาก “สถานเอก อัครราชทูตอิสราเอลประจำประเทศไทย” ให้เป็นหนึ่งในสื่อมวลชนจากเพียงไม่กี่ประเทศไปร่วมเรียนรู้จากงานนี้อีกด้วย

ในปี 2564 มีการโจมตีของแรนซัมแวร์เกิดขึ้นทุกๆ 11 วินาที เมื่อเทียบกับทุกๆ 39 วินาที ในปี 2562 โดยการโจมตีทางไซเบอร์ ในปี 2564 นั้น เกือบครึ่งพุ่งเป้าที่ธุรกิจขนาดเล็กและขนาดกลาง มูลค่าความเสียหายสูงถึง 2 หมื่นล้านดอลลาร์ และการโจมตียังเพิ่มขึ้นถึง 400 เปอร์เซ็นต์ ในช่วงการระบาดใหญ่ของโควิดในปี 2564 โดยค่าใช้จ่ายเฉลี่ยในการกู้คืนระบบอยู่ที่ 1.85 ล้านดอลลาร์ หรือราว 66.6 ล้านบาท เพิ่มจากปี 2562 กว่า 2 เท่า ยังคาดว่าความเสียหายที่เกี่ยวข้องกับไซเบอร์จะสูงถึง 10.5 ล้านล้านดอลลาร์ต่อปีภายในปี 2568 ขณะที่การใช้งบประมาณด้านความปลอดภัยทางไซเบอร์อาจสูงถึง 172 พันล้านดอลลาร์ทั่วโลกในปี 2565

หนึ่งในบุคคลสำคัญที่ขึ้นกล่าวปาฐกถาในงานได้แก่ นายเบนนี แกนต์ซ รมว.กลาโหมอิสราเอล ที่กล่าวสรุปการเปลี่ยนแปลงของความขัดแย้งในโลกไซเบอร์ที่เพิ่มมากขึ้นและรุนแรงมากขึ้น ขณะเดียวกันยังย้ำถึงความจำเป็นที่บริษัทเอกชนจะต้องปฏิบัติตามแนวทางของรัฐบาลและให้ความร่วมมือเพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้น พร้อมยังระบุอย่างชัดเจนด้วยว่า “อิหร่าน” เป็นผู้เล่นคนสำคัญที่ดำเนินการโจมตีผ่านไซเบอร์ ซึ่งแต่เดิมถือเป็นความท้าทายระดับโลกและต่อมาเป็นความท้าทายของภูมิภาค กระทั่งท้ายที่สุดเป็นภัยคุกคามต่ออิสราเอล

ส่วนไฮไลต์สำคัญในวันเปิดงานวันแรกเป็นคิวของ นายนาฟทาลี เบ็นเน็ตต์ นายกรัฐมนตรีในวันนั้น ซึ่งปัจจุบันก้าวลงจากตำแหน่งหลังทำหน้าที่ได้เพียงปีเดียวและประกาศยุบสภา เตรียมจัดเลือกตั้งทั่วไปครั้งที่ 5 ในรอบ 3 ปีครึ่ง และส่งไม้ต่อให้นายยาอิล ลาพิด รมว.ต่างประเทศ รับหน้าที่รักษาการนายกรัฐมนตรี โดยเบ็นเน็ตต์ย้ำถึงความ สำคัญของความร่วมมือกันระดับโลกเพื่อรักษาความปลอดภัยในโลกไซเบอร์ โดยเฉพาะการแบ่งปันความรู้และประสบการณ์กับมิตรประเทศ และออกปากเตือนว่า อิสราเอลไม่เคยมีนโยบายสร้างความเสียหายหรือระรานใครก่อน แต่หากผู้ใดก็ตามที่พยายามโจมตีทางไซเบอร์กับอิสราเอลจะต้อง “รับผลจากการกระทำนั้น”

เบ็นเน็ตต์ยังกล่าวด้วยว่า “โลกไซเบอร์กลายเป็นมิติของการทำสงครามในอนาคต แทนที่จะต้องส่งกองกำลังทหารไปเสี่ยงชีวิตเสียเลือดเนื้อสู้ศึกภายนอก ก็เพียงใช้กลุ่มคนจำนวนหนึ่งต่อสู้อยู่หลังคอมพิวเตอร์ที่ใดก็ได้ในโลกโดยไม่ต้องเสี่ยงชีวิต”

ก่อนจบปาฐกถาเบ็นเน็ตต์ยังให้คำแนะนำแก่ผู้เข้าร่วมฟังเต็มออดิทอเรียมซึ่งส่วนใหญ่เป็นซีอีโอ ผู้บริหารองค์กร ผู้เชี่ยวชาญ ไปจนถึงตัวแทนจากหน่วยงานต่างๆ จากทั่วโลกว่า เมื่อตัดสินใจทำสิ่งใดแล้วต้องลงมือทำอย่างฉับไว ไม่โลเล รวมทั้งพยายามหาหนทางเพื่อให้ได้รับข้อมูลที่ถูกต้องแท้จริง และสุดท้ายอย่าเล่นการเมือง.

jns Jewish News Syndicate

Israel National Cyber Directorate announces national 'cyber-dome'

The "proactive defense" will use a big-data and artificial intelligence approach to "synchronize nation-level, real-time detection, analysis and mitigation of threats," says National Cyber Directorate head.

(June 28, 2022 / JNS) Israel's National Cyber Directorate is promoting the formation of a "cyber dome," its director general said on Tuesday.

Speaking at Tel Aviv University's annual Cyber Week conference, Gaby Portnoy outlined the make-up of the dome, saying it featured a new, big-data and artificial intelligence approach to "proactive defense" against cyber threats.

According to the Directorate, some 1,500 attacks were thwarted by its teams in the past year.

"There is no longer only one type of ... enemy," said Portnoy. "On one hand, Iran has become our dominant rival in cyber, together with Hezbollah and Hamas. We see them, we know how they work, and we are there," he added.

On the other hand, he continued, the range of attackers had expanded, and now included hacker collectives, proxies, independent criminal organizations and even private individuals.

"The cyber-dome will elevate national cyber-security by implementing new mechanisms in the national cyber perimeter, reducing the harm from cyber-attacks at scale," said Portnoy.

"The cyber-dome will also provide tools and services to elevate the protection of the national assets as a whole. ... It will synchronize nation-level, real-time detection, analysis and mitigation of threats," he added.

Effective cyber security, he said, was a cooperative effort.

"You cannot fight cyber aggression alone. You have to have partners, at home, in your defense community, in the government, in the different sectors, in the academy, in the private sector and around the world," said Portnoy.

jns Jewish News Syndicate

Israeli defense minister accuses Iran, Hezbollah of trying to hack UNIFIL

Iran and Hezbollah attempted to steal materials about UNIFIL activities and deployment in the area, says Israeli Defense Minister Benny Gantz.

(June 30, 2022 / JNS) Israel's defense minister said on Wednesday that Iran and Hezbollah had attempted to hack the United Nations peacekeeping force in Lebanon, and threatened retaliation.

Speaking at Tel Aviv University's annual Cyber Week conference, Gantz said, "Iranian security institutions in cooperation with Hezbollah [recently] launched a cyber operation with the aim of stealing materials about UNIFIL activities and deployment in the area, for Hezbollah's use," according to Reuters.

"This is yet another direct attack by Iran and Hezbollah on Lebanese citizens and on Lebanon's stability," he said.

In response to Gantz's announcement, UNIFIL said that it was aware of the Israeli defense minister's remarks, but had not yet received any direct information regarding the matter, according to Reuters.

jns Jewish News Syndicate

Bayer to establish cyber-security hub in Israel

The pharma giant plans to integrate the hub into Bayer's global cyber unit. Local center to be one of the largest internal cyber units the multinational conglomerate operates.

(July 3, 2022 / Israel Hayom) Pharma giant Bayer has announced plans to establish a cyber-security hub in Israel, which will be integrated into Bayer's global cyber unit and will be one of the largest internal units of this kind in the company.

A delegation of top Bayer executives arrived in Israel on June 26 for a three-day visit, meeting with Economy and Industry Ministry Director General Ron Malka to discuss the German company's plans to deep-dive into the Israeli market.

The delegation included, among others, Bijoy Sagar, Bayer's chief information technology and digital transformation officer, and Gary Harbison, head of cyber-security and risk management, who were the driving force behind the move. The two also spoke at the main plenary of Cyber Week 2022, the annual international cybersecurity expo hosted by Tel Aviv University.

"I am excited by the spirit of innovation, level of talent and pragmatism I witnessed in the startup ecosystem, the government and universities in Israel in the sphere of information technology," said Sagar. "Bayer business in Israel is strong and the cybersecurity bub is another great addition to our initiatives in Israel."

During Cyber Week, top TAU and Bayer executives also inked a cooperation agreement to promote groundbreaking cybersecurity research from Tel Aviv University.

Subscribe to The JNS Daily Syndicate by email and never miss our top stories

Your email

"As a company engaged in R&D in the core areas of life sciences, the ability to integrate with Israel's unique cyber-security ecosystem, alongside sectors such as medical innovation and agricultural development is an opportunity to integrate as players in the Israeli market and provide added value for Bayer and for the ecosystem," said Hugo Hagen, managing director of Bayer Israel.

"As a Norwegian who has worked in Israel for three years, I feel a mission to promote Israel on Bayer's investment map and to strengthen the company's position within Israel, as well as that of the Israeli headquarters within the global headquarters," said Hagen.

"The ecosystem here is impressive and it would be a mistake not to try to enjoy the possibilities that exist here, and of course, I am proud that the decision was made to establish the new cyber-security unit here," he added.

"There is no doubt that such initiatives contribute to employment, innovation and Israel's image, and attract other international investments," noted Malka. "We will continue to represent the best Israeli innovation has to offer and link it to leading companies. We welcome Bayer's expansion in Israel and we are working to develop future similar initiatives."

Yael Mor, who will run the hub for Bayer, said, "It is exciting to create something the activities of which will have an impact in the world beyond Israel's borders. Along with our focus on the cyber unit, we will engage in locating Israeli innovation in cyber security."

Bayer is one of the largest pharmaceutical and life sciences conglomerates in the world. Its main areas of business include consumer health-care products, agricultural chemicals and biotechnology products. The company set up its offices in Israel in 2008 and currently employs 150. Worldwide, Bayer maintains a presence in 83 countries, employing some 100,000 people.

jns Jewish News Syndicate

Iranian cyber-attackers trying, and so far failing, to create panic in Israel

Observers say Iranian-Israeli cyber war has seen Iranians employ "opportunistic loopholes" • Advent of quantum computing could see new capabilities surface in cyber domain.

(June 24, 2022 / JNS) Iranian cyber-attackers targeting Israel have focused on trying to create panic; however, they have not activated advanced cyber-attack capabilities, say observers in Israel while cautioning that the hostile actors will continue to search for new vulnerabilities.

This month, Iranian cyber-attackers reportedly activated rocket sirens belonging to municipal authorities in Jerusalem and Eilat, as well as targeting the emails of senior Israeli and American officials and executives.

In November, a series of cyber strikes targeted Iranian gas stations and highway signs across the country, reportedly disabling every gas station in the country, while hijacking displays and screening subversive anti-regime messages.

As such, it appears as if the Israeli-Iranian shadow cyber war has no end in sight. Israel's National Cyber Directorate, set up in 2012 (originally known as the National Cyber Bureau), is a regulator that ensures that critical private- and public-sector websites are protected, and defines the minimum levels of protection needed for all critical infrastructure and private-sector companies.

"Specifically, the hacks targeted public-address systems in Jerusalem and Eilat," said Omree Wechsler, a senior researcher at the Blavatnik Interdisciplinary Cyber Research Center, at Tel Aviv University. "As a clear Israeli symbol, it shows that this is an opportunistic attack, and not a sophisticated and well-planned attack launched years ago; the hackers attacked where they found loopholes."

"Since many cyberattacks in the world are focused on financial or espionage targets, the Iranian activity against Israel is in accordance with the pattern of causing damage or creating panic. Such attacks are common and part of a daily routine that includes thousands of attempts to hack into any system or server whose damage would cause media coverage, in contrast to the espionage activity that also takes place every day," he stated.

'Room for improvement in all of the spheres'

Professor Col. (res.) Gabi Siboni, an expert on cyber security, military strategy and technology at the Jerusalem Institute for Strategy and Security, told JNS he assesses that "Israel has a well-oiled system for dealing with these threats and which maintains readiness. Of course, there is no immunity, and it is always possible for the attackers to locate a breach and enter through it."

Siboni, who serves as a senior consultant to the Israel Defense Forces and other Israeli security organizations, said it was important to remember that "it is not just government systems that can be attacked—civilian systems can be harmed, and significant damage can be caused," he noted, referring to the 2020 ransomware attack on the Israeli insurance company Shirbit, which proved highly damaging.

"Although the Israeli state defense system also touches on civilian systems, the civilian sphere is independent and more sensitive," he said. "There is always room for improvement in all of the spheres."

Gabi Siboni. Credit: Courtesy.

Wechsler said that when evaluating Israel's readiness for these kinds of attacks and in the wider context of Iranian cyber attacks, "it is important to draw a line between the defenses applied to military systems and installations; critical infrastructure, of which Israel was the first nation to acknowledge the importance of protecting in cyberspace; and the situation in the private sector and the local municipalities. Critical infrastructure, the attacking of which can cause physical damage, is subject to the direction of the National Cyber Directorate and is therefore well-protected."

He said "the same is true for military and national security systems. These attacks on the municipal address systems indicate a gap in awareness, regulation and enforcement when it comes to the cyber security of these entities. The same is true for many private organizations, especially small and medium businesses, where there is no agency that can enforce and oversee security procedures."

Asked to comment on reports in the international media on alleged Israeli cyber-offensive operations against Iran, Siboni said he is seeking to understand Israel's overall strategy in this campaign. "Two sides exchange blow, back and forth, but what is the strategy in this context? I always this question, and here I don't know what the answer is," he acknowledged.

According to Wechsler, "Israel is considered to be a sophisticated cyber actor across all domains, such as cyber defense and intelligence collection, and having a flourishing local cyber ecosystem. From what was revealed through the years, Israel also ranks very high in offensive cyber capabilities and has demonstrated much more advanced capabilities than Iran in that field."

"While we can certainly assume an extensive use of these capabilities for intelligence-gathering, disrupting attacks from [reports on the] Stuxnet [cyber attack on Iranian centrifuge machines] in 2010 to the attack that targeted the Shahid Rajai port in Bander Abbas [Iran] in May 2020 show that Israel allegedly uses its capabilities to disrupt and degrade Iran's nuclear plan, which Israel views as an existential threat," said Wechsler. "We cannot rule out the sabotage of other [Iranian] plans, such as ballistic missiles and advanced drones, and [Israeli] retaliation against attacks that targeted its own critical infrastructure."

Looking ahead, both Siboni and Weschler agreed that quantum computing would represent breakthroughs in cyber-warfare capabilities.

"Capabilities are always developing, for attackers and defenders," said Siboni. "I do not see a major breakthrough unless we get into the exotic area of quantum computing, which will likely happen in the foreseeable future. Until then, each side will improve incrementally, finding weaknesses and acting on them."

Wechsler said that "advances in cyber threats and capabilities are bidirectional."

"On the one hand," he explained, "it is no secret that states invest many resources in order to develop more advanced capabilities to apply for intelligence-gathering and as part of their militaries' toolbox. On the other hand, the more digital and connected we become, the more susceptible we are to these threats. Trends such as 'connect everything' and the Internet of Things (IoT) expand the attack surface, whereas emerging or future technologies, such as artificial intelligence and quantum computing are expected to boost both defensive and offensive capabilities by adding more computation power and automation."

However, the same technologies could, he assessed, also boost security, adding that "with the right regulations, principles and norms, we could also mitigate many of the risks."

MIRAGE news

Cyber Week 2022 at Tel Aviv University: Combating 'Real and Growing' Threats

Cyber Week, one of the top cybersecurity events in the world, is making a full return to Tel Aviv University campus in its usual in-person format on June 27th – 30th.

With thousands of attendees from more than 80 countries, including top CISOs and government decision makers from around the globe, this year's conference offers a thought-provoking exchange of knowledge, methods, and ideas on burning topics like fraud, crypto, cloud, the supply chain, cybersecurity for aviation, maritime, automotive, data protection, capacity building, the future cyber landscape and more.

The events will run for a full week and include over 40 roundtables, panels, workshops, forums, competitions, and more.

Pressing Need for Cyber Security Solutions

Cybercrime has never been a bigger threat than it is now, with a 600% increase in malicious emails since the beginning of the pandemic and related damage predicted to hit $10.5 trillion annually by 2025.

Furthermore, since the outbreak of Russia's war on Ukraine, cyber experts have seen a dramatic and concerning rise in cyber warfare activity, with a sustained and ongoing conflict which still threatens to escalate dramatically.

It has become increasingly important as a result, to inspire innovation and effective cyber security solutions in the industry. Major Gen (Ret) Prof. Issac Ben Israel Head of the Blavatnik Interdisciplinary Cyber Research Center and Chairman of the Conference stresses, "Cyber is an increasingly vulnerable space that is affecting everyone. Businesses must wise up to the real and growing threat of cyber-attacks, and cybersecurity experts must be ready to respond to the escalating demand for cyber security with novel solutions. We must prepare now to be ready for what we know tomorrow will inevitably hold."

Cyber Week's events span a wide variety of topics dealing with all aspects of the issue, including regulation and law, startup innovation, artificial intelligence, financial technologies, healthcare and cyber defense, and aims to inspire innovation, drive solutions and encourage collaboration.

Israeli outgoing Prime Minister Naftali Bennett spoke at last year's Cyber Week conference at Tel Aviv University

Experts from Near and Far

The Conference is now in its 12th year, and its Main Plenary Event (held from June 28th to June 29th) is the largest and most anticipated event of Cyber Week each year, during which some of the most renowned names in the cyber

world will discuss crucial dilemmas and issues facing the public and private sectors of every company, city, and country in the world today.

This year's speakers include: Outgoing Prime Minister of Israel Naftali Bennett; Benjamin Gantz, Israel Minister of Defense; Anne Neuberger, Deputy Assistant to the President & Deputy National Security Advisor for Cyber & Emerging Technologies, White House, USA; Chris Inglis, National Cyber Director of the Executive Office of the US President; Gaby Portnoy, the Director General of the Israel National Cyber Directorate; Maj. Gen. (Ret.) Prof. Isaac Ben-Israel, Conference Chairman of Cyber Week and Director of Blavatnik Interdisciplinary Cyber Research Center at the Tel Aviv University; Jane Horvath, Chief Privacy Officer of Apple, Inc.; Lindy Cameron, CEO of the National Cyber Security Center; Tim Brown, CISO of SolarWinds; Cecilie Fjellhøy, Founder of action:reaction, Netflix-star Tinder Swindler; Jason Chan; Former VP, Information Security of Netflix and many more.

Cyber Week is hosted by the Blavatnik Interdisciplinary Cyber Research Center and the Yuval Ne'eman Workshop for Science, Technology and Security, at Tel Aviv University, headed by Major Gen. (Ret.) Prof. Isaac Ben-Israel, together with the National Cyber Directorate at the Prime Minister's Office, The Ministry of Economy and Industry and the Ministry of Foreign Affairs.

MIRAGE news

Tackling Worrying Rise in Cyber Crimes and Warfare

Israel's 12th Annual Cyber Week Conference was attended last week by 300 speakers, 7000 in person and 2000 online attendees from 80 countries. The speakers included top Israeli government figures such as then Prime Minister Naftali Bennett and Defense Minister Benny Gantz; leading American and British cyber figures, including Chris Inglis, the National Cyber Director at the Executive Office of the President at the White House and Lindy Cameron CEO of the British National Cyber Security Centre, and security executives from large companies, such as Walmart, SolarWinds,Apple and Netflix.

TAU researchers presented different academic perspectives on cybersecurity challenges, demonstrating the broad interdisciplinary scientific research on cybersecurity at TAU: Prof. Eran Toch from the Department of Industrial Engineering on "The Science of Cybersecurity in Organizations: Why is it so hard and what it takes to do it right"; Prof. Niva Elkin-Koren from The Buchmann Faculty of Law on "Digital Surveillance: Rethinking the Design Approach" and Prof. Yehuda Afek from the Blavatnik School of Computer Science on "Securing the DNS System."

This year's gathering took place against the backdrop of unprecedented cyber challenges and events including Russia's war on Ukraine. Speakers described a dramatic and concerning rise in cyber warfare as well as cybercrime – cyber-related damage is predicted to hit $10.5 trillion annually by 2025, while cybersecurity spending on data

protection and risk management could reach $172 billion globally in 2022. Yet they also expressed hope in the effectiveness of properly implemented defenses and evolution in defensive cyber techniques to meet the challenge.

The Human Aspect of Cyber

Ira Winkler, CISSP, Chief Security Architect of Walmart, outlined the important role government plays saying, "at a high level, governance tells people how to do things correctly with cyber security at the forefront." He also recognized the need to account for the human aspect of cyber and to be realistic when devising and implementing strategy, "A user is as much as part of the system as a computer. Stop expecting people not to click on suspicious content, but rather have a strong network protecting them."

The human face of fraud victims was highlighted through Norwegian Netflix star, Cecilie Fjellhøy, from "Tinder Swindler," who was scammed of hundreds of thousands of US dollars by a man she knew as Simon Leviev. Fjellhøy uses her own experience to fight for justice for fraud victims around the world, and discussed the subject of "the day after" for those affected and what we as a society can learn from it.

Cecilie Fjellhøy from "Tinder Swindler used her own experience to speak up for fraud victims (Photo: Chen Galili)

In contrast, self-professed "Hacker, Helper and Human," Jason E. Street, VP Infosec, Sphere NY, USA, illustrated weak points – human factors were highlighted – of companies and institutions with regard to security breaches. Street showed video footage of himself strolling into banks and compromising their security on the highest level in next to no time. He reminded those in the audience who were shaking their heads and laughing that their companies could be next in line, and urged them to prepare for such a scenario.

Terrorists with Keyboards

Israel's former Prime Minister Naftali Bennett pointed out how "inevitably cyber is going to become one, if not the most, prominent dimensions of future warfare," while drawing attention to the vital need for global collaboration in the cyber sphere. In cyber, he reasoned, the same actors who attack one company or country are often attacking others at the same time. Information sharing can help all vulnerable parties defend themselves.

Israel's Minister of Defense, Benny Gantz, outlined the increasing shift of conflicts to the cybersphere, noting that bad actors are already carrying out cyberattacks, particularly Iran. The country uses new [cyber] proxies, who Gantz referred to as "terrorists with keyboards," in addition to their direct actions. He stressed the need for private companies to follow government guidelines and cooperate on a response, stressing that "Iran is first a global challenge, then it is a regional challenge, and only finally is it a threat to the State of Israel. The same goes for the cyber dimensions – the same framework of cooperation vis-a-vis Iran is expanding to cyber."

themedialine
worthy mideast news tm

Israel Presents Cyber Dome Defense at International Forum in Tel Aviv

We are creating a global cybersecurity collaboration network, PM Bennett says

The Cyber Dome, a big data, artificial intelligence approach to proactive defense, "will elevate national cybersecurity by implementing new mechanisms in the national cyber perimeter, reducing the harm from cyberattacks at scale," Gaby Portnoy, the director-general of the Israel National Cyber Directorate (INCD), said on Tuesday.

Portnoy spoke as he presented the organization's newest project at the June 27-30 Cyber Week 2022 event held at Tel Aviv University by the INCD and the university's Blavatnik Interdisciplinary Cyber Research Center.

The Cyber Dome name was chosen to draw a parallel to Israel's successful Iron Dome air defense system.

Cyber is going to become one, if not the most prominent dimension, of future warfare

Israeli Prime Minister Naftali Bennett pointed out at the event that inevitably, "cyber is going to become one, if not the most prominent dimension, of future warfare."

He continued, "Collaboration is always a beautiful word, but in cyber it's vital because the same bad guys who are attacking one company, or one country are attacking at the same time a bunch of other countries. And if you can share that information, then everybody else can defend themselves."

Israel is investing in creating a global collaboration network in the cybersecurity arena together with its allies, Bennett said. "It's vital and we are going to pursue that," he continued.

Anne Neuberger, the American deputy national security adviser for cyber and emerging technology, pointed out during her speech at the conference the main reasons the US is investing in cooperation with its allies on cybersecurity.

First, working together reinforces the trust and communication across countries, she stressed. Also, Neuberger continued, various "malicious attackers use many of the same techniques, so sharing information enables each of us to better protect against emerging threats."

Lastly, she added that the international community can build norms and practices as the world has in other domains to maintain stability and prevent conflict.

This is our vision, Neuberger said, "like-minded countries working together to ensure that the global community can gain the benefits of cyberspace and avoid the harms."

Collaboration, cooperation, and integration is the way forward

Dr. Melanie Garson, cyber policy lead for Europe, Israel, and the Middle East at the Tony Blair Institute for Global Change, told The Media Line that cybersecurity is not a solo endeavor.

J-Wire

"Collaboration, cooperation, and integration is the way forward," she said.

Garson added that for most countries, the greatest security threat is the perception that they are not at risk, leaving them as "low hanging fruits for cybercriminals, state-backed or not, to pick up."

Israel in particular, she noted, has always lived in the perception of threat. "They have tightened their defenses because of the experience of threat," she said.

Srdjan Rajcevic, minister of scientific and technological development, higher education, and information society in the Republika Srpska government, in Bosnia and Herzegovina, said his country seeks to further collaborate with Israel.

"Currently we are seeking to cooperate more with the State of Israel in terms of sharing experience and threat intelligence. We want to acquire the defense mechanism and know-how from the Israelis so that we can be better prepared for cyber incidents," he told The Media Line.

To this end, said Rajcevic, they are cooperating with ELTA Systems, a subsidiary of Israel Aerospace Industries, to establish the first cyber academy in the Republic of Srpska.

"Cyberwarfare is a reality, and we need to be aware of this. And if we know that cyberwarfare is here to stay, we need to be prepared," Rajcevic stressed.

Ari Uusikartano, deputy director-general for information and documentation at the Finnish Foreign Ministry, discussed the importance of international cooperation on cybersecurity in an interview with The Media Line.

Cyber knows no limits, borders, or barriers, he said. "That is why he must have the ability to exchange information, interact, and also face the threats together. Cyber does not limit itself within the nation-state," he said.

He added that Finland, as well as the European Union, is worried by cyberthreats coming from Russia in the context of the invasion of Ukraine and stressed the need for the EU to increase cooperation to counter these threats.

Bruno Gencarelli, head of the unit for international data flows and protection at the European Commission, said cybersecurity has become such an important issue because of the evolution of technology and of threats.

In a digital world, "crime has also become digital and borderless and that's also why we need to cooperate on these threats," Gencarelli told The Media Line.

Cybersecurity is now an essential part of the EU's cooperation with all of its closest partners, "on the other side of the Atlantic, here in this region [the Middle East], including Israel of course, with countries in the Asia-Pacific area," he added.

"It is now an integral policy to our bilateral relationships with many countries that are facing the same threats. Israel has of course the expertise, the know-how which is in the top class in the world," Gencarelli said.

Australian professionals attend Israel Cyber Week

The Israel Trade and Economic Commission in Sydney and the Trans-Tasman Business Circle have taken a business delegation of 18 cyber security professionals from Australia and New Zealand to Tel Aviv.

The delegation was led by cyber security professional Alistair MacGibbon.

Israel Cyber Week was held between June 27and June 30 and attracted more than 9,000 attendees from more than 80 countries, and showcased the latest tech in the rapidly-changing world of cyber security.

Israel's former Prime Minister, Naftali Bennett, was interviewed on stage by Microsoft Israel's CEO Michal Braverman-Blumenstyk, while moments earlier, the Australian and New Zealand Delegation to Israel Cyber Week was lauded as the first-ever in-person delegation from the region.

Mike Rodgers, former National Security Agency Director and Australian Ambassador to Israel Paul Griffiths addressed the delegation.

Alistair MacGibbon, CSO at CyberCX, joined an illustrious panel, expounding their thoughts on the global cyber security world in 2030. The panel and former Prime Minister Bennett spoke about geopolitical issues, including the Iranian threat and the Russian- Ukrainian war, through the lens of state-based actors attacking critical infrastructure and sovereign entities.

The Israel Trade and Economic Commission's Jeremy Ungar is responsible for cyber security. He said: "A small and dynamic group of cyber professionals became instant friends and gained a wealth of knowledge that supersedes Zoom meetings and introductions".

The value achieved with the Australian-New Zealand outbound delegation to Israel for Cyber Week is already tangible with sign-ups for the next Israel Cyber Week delegation already registered.

CISION
PR Newswire

Israel's 12th Annual Cyber Week Highlights Unprecedented Changes in the Cyber Landscape and the Critical Need For Coordinated Response

TEL AVIV, Israel, June 29, 2022 /PRNewswire/ -- Top Israeli government figures such as Prime Minister Naftali Bennett and Defense Minister Benny Gantz, addressed the conference which is headed by Maj. Gen. (Ret.) Prof Isaac Ben-Israel, known as the "father" of the Israeli Cyber industry. Leading American and British cyber officials also contributed, including Chris Inglis the National Cyber Director at the Executive Office of the President at the White House, Anne Neurberger the Deputy Assistant to the US President and Deputy National Security Advisor for Cyber and Emerging Technologies at the White House, and Lindy Cameron CEO of the National Cyber Security Centre. Private sector leaders including Ira Winkler, Chief Security Officer for Walmart, Tim Brown CISO of SolarWinds, Jane Horvath, Chief Privacy Officer of Apple, Jason Chan, Former VP of Information Security at Netflix, also addressed the conference. Supported by Israel's Ministry of Economy and Innovation, attendees joined from over 80 countries from all over the world. Guests included startups and major investors, together with numerous sponsors, and partners.

Cyber Week is jointly held by the Blavatnik Interdisciplinary Cyber Research Center (ICRC); The Yuval Ne'eman Workshop for Science, Technology and Security at Tel Aviv University; and the Israeli National Cyber Directorate under the Prime Minister's Office. The gathering occurred against the backdrop of unprecedented cyber challenges and events including Russia's war on Ukraine. Speakers described a dramatic and concerning rise in cyber warfare as well as cybercrime - cyber-related damage is predicted to hit $10.5 trillion annually by 2025, while cybersecurity spending on data protection and risk management could reach $172 billion globally in 2022. Yet they also expressed hope in the effectiveness of properly implemented defenses and evolution in defensive cyber techniques to meet the challenge.

Israel's Prime Minister Naftali Bennett pointed out how "inevitably cyber is going to become one if not the most prominent dimensions of future warfare," while drawing attention to the vital need for global collaboration in the cyber sphere saying, "In cyber it's [collaboration] vital because the same bad guys who are attacking one company or country are attacking others at the same time. If you can share that information everyone else can defend themselves. It's like a pickpocket in a subway and if someone sprays them with red paint everyone can see and defend themselves."

Ira Winkler: CISSP, Chief Security Architect, Walmart outlined the important role government plays saying, "at a high level, governance tells people how to do things correctly with cyber security at the forefront." He also recognized the need to account for the human aspect of cyber and to be realistic when devising and implementing strategy, "A user is as much as part of the system as a computer. Stop expecting people not to click on suspicious content, but rather have a strong network protecting them."

Israel's Minister of Defense, Benny Gantz, outlined the increasing shift of conflict to the cybersphere and that bad actors are already carrying out attacks via cyber, particularly Iran. The country uses "new [cyber] proxies [who] "are terrorists with keyboards," in addition to their direct actions. In response, Defense Minister Gantz stressed the need for private companies to follow government guidelines and cooperate saying, "Iran is first a global challenge, then it is a regional challenge, and only finally is it a threat to the State of Israel. The same goes for the cyber dimensions and the same framework of cooperation vis-a-vis Iran is expanding to cyber."

About CyberWeek:

Cyber Week is a leading international cybersecurity event that provides a unique opportunity for experts from industry, government, military and academia to share their knowledge about the challenges and opportunities in the field. Cyber Week is hosted by the Blavatnik Interdisciplinary Cyber Research Center and the Yuval Ne'eman Workshop for Science, Technology, and Security, at Tel Aviv University, headed by Major Gen. (Ret.) Prof. Isaac Ben-Israel together with the National Cyber Directorate at the Prime Minister's Office, The Ministry of Economy and Industry, and the Ministry of Foreign Affairs.

TEL AVIV UNIVERSITY
Pursuing the Unknown

Tackling a Worrying Rise in Cyber Crimes and Warfare

Israel's 12th annual Cyber Week highlights critical need for coordinated response

Israel's 12th Annual Cyber Week Conference was attended last week by 300 speakers, 7000 in person and 2000 online attendees from 80 countries. The speakers included top Israeli government figures such as then Prime Minister Naftali Bennett and Defense Minister Benny Gantz; leading American and British cyber figures, including Chris Inglis, the National Cyber Director at the Executive Office of the President at the White House and Lindy Cameron CEO of the British National Cyber Security Centre, and security executives from large companies, such as Walmart, SolarWinds,Apple and Netflix.

TAU researchers presented different academic perspectives on cybersecurity challenges, demonstrating the broad interdisciplinary scientific research on cybersecurity at TAU: Prof. Eran Toch from the Department of Industrial Engineering on "The Science of Cybersecurity in Organizations: Why is it so hard and what it takes to do it right"; Prof. Niva Elkin-Koren from The Buchmann Faculty of Law on "Digital Surveillance: Rethinking the Design Approach" and Prof. Yehuda Afek from the Blavatnik School of Computer Science on "Securing the DNS System."

This year's gathering took place against the backdrop of unprecedented cyber challenges and events including Russia's war on Ukraine. Speakers described a dramatic and concerning rise in cyber warfare as well as cybercrime - cyber-related damage is predicted to hit $10.5 trillion annually by 2025, while cybersecurity spending on data protection and risk management could reach $172 billion globally in 2022. Yet they also expressed hope in the effectiveness of properly implemented defenses and evolution in defensive cyber techniques to meet the challenge.

The Human Aspect of Cyber

Ira Winkler, CISSP, Chief Security Architect of Walmart, outlined the important role government plays saying, "at a high level, governance tells people how to do things correctly with cyber security at the forefront." He also recognized the need to account for the human aspect of cyber and to be realistic when devising and implementing strategy, "A user is as much as part of the system as a computer. Stop expecting people not to click on suspicious content, but rather have a strong network protecting them."

The human face of fraud victims was highlighted through Norwegian Netflix star, Cecilie Fjellhøy, from "Tinder Swindler," who was scammed of hundreds of thousands of US dollars by a man she knew as Simon Leviev. Fjellhøy uses her own experience to fight for justice for fraud victims around the world, and discussed the subject of "the day after" for those affected and what we as a society can learn from it.

Cecilie Fjellhøy from "Tinder Swindler used her own experience to speak up for fraud victims (Photo: Chen Galili)

In contrast, self-professed "Hacker, Helper and Human," Jason E. Street, VP Infosec, Sphere NY, USA, illustrated weak points - human factors were highlighted - of companies and institutions with regard to security breaches. Street showed video footage of himself strolling into banks and compromising their security on the highest level in next to no time. He reminded those in the audience who were shaking their heads and laughing that their companies could be next in line, and urged them to prepare for such a scenario.

Terrorists with Keyboards

Israel's former Prime Minister Naftali Bennett pointed out how "inevitably cyber is going to become one, if not the most, prominent dimensions of future warfare," while drawing attention to the vital need for global collaboration in the cyber sphere. In cyber, he reasoned, the same actors who attack one company or country are often attacking others at the same time. Information sharing can help all vulnerable parties defend themselves.

Israel's Minister of Defense, Benny Gantz, outlined the increasing shift of conflicts to the cybersphere, noting that bad actors are already carrying out cyberattacks, particularly Iran. The country uses new [cyber] proxies, who Gantz referred to as "terrorists with keyboards," in addition to their direct actions. He stressed the need for private companies to follow government guidelines and cooperate on a response, stressing that "Iran is first a global challenge, then it is a regional challenge, and only finally is it a threat to the State of Israel. The same goes for the cyber dimensions - the same framework of cooperation vis-a-vis Iran is expanding to cyber.

Then Israeli Prime Minister Naftali Bennett speaks at Cyber Week 2022 conference at Tel Aviv University (Photo: Chen Galili)

About Cyber Week

Cyber Week is a leading international cybersecurity event that provides a unique opportunity for experts from industry, government, military and academia to share their knowledge about the challenges and opportunities in the field. Cyber Week is jointly held by the Blavatnik Interdisciplinary Cyber Research Center (ICRC); The Yuval Ne'eman Workshop for Science, Technology and Security at Tel Aviv University; and the Israeli National Cyber Directorate under the Prime Minister's Office.

THE TIMES OF INDIA

Israel focuses on training next-gen to drive its cyber systems

Bharti Jain / Updated: Jul 6, 2022, 17:28 IST

SHARE AA

ARTICLES

- Israel focuses on training next-gen to drive its cyber systems
- Shielding up: Why cybersecurity is a booming industry
- Explainer: Can Netanyahu regain Israel's premiership?
- Three Israelis, 64 Palestinians wounded in West Bank clashes

Israeli politicians with Israeli Minister of Foreign Affairs Yair Lapid (L) and outgoing Prime Minister Naftali Bennett (AFP)

TEL AVIV: As Israel continues to invest heavily in hitech innovation and R&D, the Israeli National Cyber Directorate (INCD) is working actively on advancing the next generation of human capital which will lead the field of cyber-systems, steer the Israeli cyber-industry, and leverage it in both the local and international arenas.

TEL AVIV: As Israel continues to invest heavily in hitech innovation and R&D, the Israeli National Cyber Directorate (INCD) is working actively on advancing the next generation of human capital which will lead the field of cyber-systems, steer the Israeli cyber-industry, and leverage it in both the local and international arenas.

This is being done by advancing training programs and educational projects that seamlessly integrate Israeli youth into the worlds of cyber and information security. As former Israeli Prime Minister Naftali Bennett shared at the cyber week event only a couple of days ago, "We have plenty of investment and everything, we just need more good people and we've exhausted the immediate bucket of talent".

Israel is a pioneer in the field of cyber security, having attracted 8.8 billion dollars worth of investment and 41% of the total global investments in the sector in 2021.

Much of Israel's cyber security talent pool comes from years of scouting, training and conditioning of young recruits by the Israeli Defence Forces. A background with IDF cyber defense and 8200 unit of Intelligence corps has spawned many a success story in cyber tech startups, but Israel is now looking at four different sources of new talent — Haredims, Arab women, those from the periphery and even Palestinians — according to Bennett.

Haredim, the ultra-orthodox Jewish community are exempt from mandatorily serving in the Army while they complete their religious pursuits at the yeshivas. "They're really smart and not inside of the economy. My approach wasn't popular and now it's policy, we need to provide them with an exemption for the military and let them join the workforce instead of forcing them to stay in the yeshivas until 24. It's challenging because they don't know English. It might not be the just thing, but it's the right thing," says Bennett. The move has its own critics among the Orthodox voices who see it as an attempt to drive the community away from tradition.

The second talent pool that the nation — which has built an enviable national cyber ecosystem that covers the defence forces, government agencies, private sector actively facilitated by the government, an education system that introduces cyber literacy as early as middle school and thriving start ups, many of which are driven by ex-IDF and 8200 unit of intelligence corps — is looking at is powered by Arab women whose employment levels are abysmally low. "Lots of smart Arab women we want to bring in and we're working on it. The hitech sector needs to be open to bringing in those who are different and not part of the same club," says Bennett.

The third talent pool are hi-tech professionals from the periphery areas outside of Tel Aviv like Haifa, Jerusalem and Beersheba (the desert

The third talent pool are hi-tech professionals from the periphery areas outside of Tel Aviv like Haifa, Jerusalem and Beersheba (the desert town of Beersheba, incidentally, is already the new cyber tech hub with the defence units, Cert-IL, start up coordinator Cyber 7 and Ben Gurion University located there). "It's only 40 minutes away. For many years the north and south were underserved and it's just stupid policy of Israel and when I was minister I pushed to give them access to 5 unites math. We're working hard in 11th and 12th grade to bring them into 8200," Bennett told a session at the cyber week held from June 27 to 30 here.

Interestingly, Bennett has also approved the immediate joining of Palestinian employees to Israeli hi-tech, including free movement to come here.

Israel, meanwhile, is also eyeing its 1.5 lakh-strong hitech diaspora and offering them incentives to work in Israel and close the immediate shortage of trained cyber security personnel.

"Our top mission in the defence establishment is to foster this community, to train our personnel and to keep them with us. We are constantly assessing force build up in terms of human resources, training and missions," Israel defence minister Benny Gantz said while addressing the cyber week.

THE TIMES OF INDIA

Russia, China, North Korea and Iran lead in supporting aggressive cyber attackers, says HolistiCyber CEO

Bharti Jain / TNN / Updated: Jul 10, 2022, 11:04 IST

SHARE AA

ARTICLES

Russia, China, North Korea and Iran lead in supporting...

In Nomad's Land

Shinzo Abe's killing haunts Japan with questions on...

Japan votes in shadow of ex-PM Shinzo Abe assassination

TOI

TEL AVIV: Nation state-backed cyber attacks have gained currency and notoriety over the past couple of years, with Russia, China, North Korea and Iran taking the lead in actively supporting aggressive cyber attackers, according to Israeli cyber defence firm HolistiCyber CEO Ran Shahor who had started the first cyber attack programme of the

attackers, according to Israeli cyber defence firm HolistiCyber CEO Ran Shahor who had started the first cyber attack programme of the

Intelligence branch of Israeli Defense Forces (IDF) 26 years ago.

Shahor, while speaking on 'geo-political tension and national state grade attacks' at the Cyber Week held recently in Tel Aviv, shared that each of the four countries listed above had a different motivation for backing cyber attackers and hackers. Russia does it to create disorder and panic in the western world; China mainly for IP espionage; North Korea and Iran originally for terror crimes though they have now moved to simple cyber crime. Stating that both Iran and North Korea started supporting nation-state grade cyber attacks after a long list of international, tight sanctions against them, the retired IDF Brigadier General said that Russia, which over the past few months has faced similar sanctions in wake of the war on Ukraine, is also expected to move towards intensive cyber crime.

"It will affect all of us. Iran and North Korea are already there. It is fascinating to think where China is going. But there is no doubt we are expecting very challenging days going forward," he warned.

Stating that cyber crime was very profitable with no risk to the attacker, Shahor said that 12 years ago, when merely writing a firewall and anti-virus was enough, the cyber crime scene changed and the attacks became more aggressive, bold and sophisticated even as the defenders failed to react properly. Six years ago, Russian group Shadow Brokers accessed a whole lot of tech tools from NSA and started selling these on the DarkNet. In the last two years ago, nation states are increasingly using private cyber hacker groups to hit critical infrastructure and even the private sector. "Today's attacker is heavily backed, supported and even instructed by the nation states," warned Shahor. He said the proxies serve the nation states to augment large cyber attacks while maintaining own deniability. The attackers too are exposed to a different level of financing and, more importantly, to nation state methodology and technology.

The HolistiCyber co-founder said that Israel has an advantage in dealing with nation state-backed cyber attacks as unlike the rest of the world that is fighting a short supply of cyber security experts, it has a regular supply of manpower as each year 1000 of brightest girls and boys who must mandatorily serve in the Israeli army are cherry picked and trained to become cyber ninjas. Also, unlike most western countries that either do not allow cyber attacks or find them too expensive, Israel is a greenhouse for defence and offence technologies and has over 300 cyber companies. Israel has also ensured that all sectors -- the defence community, government sector, academia, private sector and international partners – work together to fight cyber aggression.

Shahor said the solution against nation state-backed cyber attacks lies in getting into the mind of the attacker; working with a team of world-class experts with a proven attacker background; adopting a holistic approach by protecting the entire supply chain and not just the IT systems; darknet access for intelligence; and automation for efficiency.

Asking defenders against nation state-grade cyber attacks to prioritise and defend what matters, while also taking calculated risks, Shahor said that while nobody can be fully protected from cyber attacks, "you must be better protected than your competition".

(The correspondent was in Tel Aviv as a guest of Israeli foreign ministry)

Time Bulletin

HOME NEWS ENTERTAINMENT TECH LIFESTYLE SPORTS CRYPTOCURRENCY NFT VIDEOS OTHER

NEWS

12th Annual Cyber Week: An international cybersecurity event hosts at Tel Aviv University in Israel

Published 1 month ago on June 28, 2022
By Raeesa Sayyad

ADVERTISEMENT
CrowdStrike®
Download the Whitepaper
Open

LATEST TRENDING VIDEOS
TECH / 7 hours ago
Step by Step guide to recording

Digital Week is a yearly international cybersecurity event hosted at Tel Aviv University in Israel. Throughout recent years, Cyber Week has become internationally acclaimed as one of the top cybersecurity events in the world.

With in excess of 9,000 attendees from in excess of 80 countries, Cyber Week is a place where cybersecurity experts, industry leaders, startups, investors, academics, diplomats, and government officials share knowledge, methods, and ideas on how companies and individuals stay safe from cybercriminals and internet bad actors.

Governments and businesses have prioritized cybersecurity, particularly during the pandemic, where cybercriminals have expanded and worked on their tactics to breach organizations in view of the mixture of work and online learning setups.

Cybercrime dramatically expanded during the pandemic.

1) Online scams spiked by over 400% in 2020 compared with earlier years.

2) Phishing emails developed significantly that Google blocked more than 18 million malware and phishing emails connected with COVID-19 day to day. This incorporates spear phishing for espionage purposes.

3) A recent study titled "The impact of COVID-19 on cybercrime and state-sponsored cyber activities" by Johannes Wigg figured out that groups of hackers accepted to be sponsored by Russia, China, and North Korea utilized personalized emails containing references to the pandemic to taint their targets with malware or steal passwords.

4) More than 90% of healthcare organizations suffered to least cybersecurity breach, as indicated by the US Healthcare Cybersecurity Market 2022 report.

Digital Week 2022 won't just assist with dealing with these issues directly, it will likewise attempt to help governments and organizations in confronting cyber dangers by presenting the most recent technologies and techniques in battling cybercriminals.

Cyber Week is held together by the Blavatnik Interdisciplinary Cyber Research Center (ICRC), The Yuval Ne'eman Workshop for Science, Technology and Security, Tel Aviv University, the Israeli National Cyber Directorate under the Prime Minister's Office, and the Ministry of Foreign Affairs is a main international conference in cybersecurity.

وكالة المغرب العربي للأنباء
MAP
AGENCE MAROCAINE DE PRESSE
The value of information

Cyber Security: Global Attention on the Rise as Cyber Attacks Escalate

Abderrazak Trebak

The need for cybersecurity to protect systems, networks and data is increasing worldwide, with the accelerating digital transformation of societies and various economic and social activities, as well as the risks of mass cyber attacks, fraud and hacking.

Recent studies reveal an alarming rise in war and cybercrime, and estimate that the associated damage will reach $10.5 trillion annually by 2025 globally.

Cyber attacks are often aimed at accessing sensitive information to steal or destroy it, disrupt networks or obtain funds.

Faced with this situation, governments and companies are opting for cybersecurity solutions to protect infrastructure, equipment, facilities, and various economic and financial systems.

"Governments are required to work more to protect networks and information systems, and to invest in cyber scientific research and human capital in order to efficiently use these tools," Ran Natanzon, Head of innovation & Country branding, Public Diplomacy Division at Ministry of Foreign Affairs of Israel, told MAP on the sidelines of a visit of a delegation of international journalists to Tel Aviv.

In Israel, cyber industry data show that in 2021, a significant number of transactions were made, reaching a record level of $8.8 billion.

For his part, Major General and mathematician Issac Ben-Israel, a pioneer in Israel's cyber-industry program, said that "with the use of the Internet, 'everything becomes exposed'. Data is visible, and funds are discovered, as well as privacy, health and security, in addition to the activities of government administrations".

He added that Israel sets itself to be "among the five major powers in the world in the field of cyberindustry and stands out as an electronic force, and that is why we have established an electronic research center in every university, and today we teach cybersecurity in secondary schools."

This interest in the cyber sector is most evident in the remarkable development of the new technological pole in the city of Beersheba in the Negev desert, which currently hosts more than 70 of the largest companies employing nearly 2,500 people, most of whom are information engineers.

Ran Natanzon indicated that the strategic plan for the coming years foresees that this center will include 15 intelligent buildings, providing about ten thousand jobs in artificial intelligence and computer engineering, and highly developed centers for research, innovation, alert and response to computer attacks, some of which will be under the supervision of specialized teams from the army.

This pole in the city of Beersheba also houses the electronic units of the army and the major Israeli companies in the field, especially the software companies CheckPoint, Nir Zuk's Palo Alto Networks, SentinelOne and Cybereason, in addition to centers of the largest international companies such as Google, Intel, and Microsoft, among others.

Ran Natason pointed out that the Beersheba center complements the others in Tel Aviv and Haifa, which aim to make Israel one of the world's leading countries in the field of cybersecurity.

He also stressed that this trend will strengthen the scientific research and development sector, which in Israel represents 5.4% of the gross domestic product (GDP) (2021), given the fact that the per capita GDP amounted to 44,214 dollars in the fourth quarter of 2021.

This rate places Israel at the top world rank in terms of scientific research and development intensity, and at the fifth world rank in modern technology density (per population), while the share of Israeli exports in the high-tech sector has reached about 54 percent in 2021.

As for the percentage of workers in the high-tech sector, it reached 10.4 percent of the total workforce in 2021.

To develop the Beersheba Center, Israel's Cyberspace Directorate provides support to companies that set up shop in the area.

From the same city, the National Cyber Directorate manages the "Iron Dome in Cyber Defense" project, which aims to monitor and track various cyber attacks that target all infrastructure in Israel.

In a statement to MAP, Roy Yarom, executive director of policy and strategy at the Israeli Department of Cybersecurity, said that the "Iron Dome in Cyber Defense" project will provide comprehensive protection of economic and administrative facilities, and even personal computers, in a way that enhances the defense of Israeli cyberspace and strengthens its structure in both shielding and confrontation.

Rom Yarom pointed out that the Internet will inevitably become one of the dimensions of future warfare, if not the most important.

He said that everyone should take cybersecurity seriously because cybercriminals target not only government agencies and private institutions, but also employees, ordinary people, and even children and minors because they are the most vulnerable sectors of society.

On the other hand, he stressed that there are promising opportunities for cooperation between Morocco and Israel in the cyber and digital field for open, reliable, secure, and stable cyberspace.

Yarom highlighted the promising opportunities for cooperation in the academic and scientific fields, research, and development, in addition to exchanging information and skills, as well as students and organizing joint research.

He stressed the importance of promoting information exchange to respond to common cross-cutting threats and to implement standards of responsible behavior in cyberspace.

In view of the significant development of the cybersecurity sector in Israel, the number of transactions it carries out and its growing attractiveness on a global scale, a regular annual international event is organized under the name of "Cyber Week", the latest edition of which was held at Tel Aviv University last June, in cooperation with the Israeli Ministry of Foreign Affairs.

The week is an international event that provides an opportunity for experts from industry, government, defense, and academia to share their knowledge on challenges and opportunities in the field, and to discuss cyberattacks, damage to countries' critical infrastructure, public spending on information technology, the pace of spending on cyber protection, and privacy infringement.

According to the results of a study presented at the last session of the conference, spending on cybersecurity for data protection and information risk management is expected to reach $172 billion worldwide in 2022.

Another study reported that cybercrime increased significantly during the Covid 19 pandemic, and online fraud increased by more than 400% in 2020 compared to previous years, and fraudulent messages dramatically doubled as Google blocked more than 18 million malicious and phishing emails during the pandemic.

This includes scams, theft as well as the implementation of malicious tracking and spyware.

وكالة المغرب العربي للأنباء MAP AGENCE MAROCAINE DE PRESSE
The value of information

Cybersécurité: Un intérêt mondial croissant face aux nombreuses cyberattaques

Abderrazak Trebak

Tel-Aviv – A travers le monde, la cybersécurité s'avère de plus en plus importante dans la protection des systèmes, des réseaux et des données, d'autant plus que l'accélération de la transformation numérique des sociétés et des diverses activités économiques et sociales, s'accompagne, le plus souvent, de risques élevés des cyberattaques, de fraude et de piratage.

Des études récentes démontrent une augmentation "alarmante" de cyber-guerre et de la cybercriminalité, estimant que les dommages y afférents atteindront annuellement les 10,5 trillions de dollars en 2025.

Les cyber-attaques visent souvent à accéder à des informations sensibles pour les voler ou les détruire, perturber les réseaux ou obtenir des fonds.

Face à ces données, les gouvernements et les entreprises optent pour des solutions de cybersécurité, dans le dessein de protéger les infrastructures, les équipements, les installations, ainsi que les différents systèmes économiques et financiers.

Dans ce sens, Ran Natanzon, directeur du Département des systèmes d'information et de l'innovation au ministère israélien des Affaires étrangères, a confié à la MAP, en marge de la visite d'une délégation de journalistes internationaux à Tel-Aviv, que "les gouvernements sont appelés à dépenser davantage pour protéger les réseaux et les systèmes d'information, et à investir dans la recherche scientifique cybernétique et le capital humain pour une exploitation efficace de ces outils".

En Israël, les données de la cyber-industrie relèvent qu'en 2021, un nombre important de transactions a été réalisé, atteignant un niveau record de 8,8 milliards de dollars.

De son côté, le major-général et mathématicien, Issac Ben-Israel, un pionnier du programme de la cyber-industrie en Israël, a indiqué qu'"avec l'utilisation d'Internet, +tout devient exposé+. Les données sont visibles, et les fonds sont découverts, au même titre que la vie privée, la santé et la sécurité, en plus des activités des administrations gouvernementales".

"Israël s'est fixé l'objectif de faire partie des cinq grandes puissances mondiales dans le domaine de la cyber-industrie et s'imposer comme une force en la matière. C'est pourquoi, nous avons établi un centre de recherche électronique dans chaque université, et aujourd'hui nous enseignons la cybersécurité dans les écoles secondaires", a-t-il mis en avant.

Ce grand intérêt pour le secteur cybernétique se manifeste clairement dans le développement remarquable du nouveau pôle technologique de la ville de Beer-Sheva dans le désert du Néguev, qui comprend actuellement plus de 70 grandes entreprises employant environ 2.500 personnes, dont la plupart des ingénieurs en informatique.

Ainsi, Ran Natanzon indique que le plan stratégique pour les années à venir prévoit que ce pôle comprendra 15 bâtiments intelligents, fournissant une dizaine de milliers d'emplois en intelligence artificielle et en ingénierie informatique, et des centres très développés de recherche, d'innovation, d'alerte et de riposte aux attaques informatiques, dont certains seront sous la supervision d'équipes spécialisées de l'armée.

Le pôle de la ville de Beer-Sheva abrite les unités électroniques de l'armée et les grandes entreprises israéliennes, notamment les éditeurs de logiciels CheckPoint, Palo Alto Networks de Nir Zuk, SentinelOne et Cybereason, ainsi que les centres des grandes entreprises internationales telles que Google, Intel, Microsoft, entre autres.

Le Centre de Beer-Sheva vient, ainsi, compléter les autres de Tel-Aviv et de Haïfa, qui visent à faire d'Israël l'un des plus grands pays du monde dans le domaine de la cybersécurité, met en relief Ran Natanzon.

Il a également souligné que cette tendance renforcera la force du secteur de la recherche scientifique et du développement, qui représente en Israël 5,4% du produit intérieur brut (2021), sachant que la part par habitant du PIB s'est élevée au quatrième trimestre de 2021 à environ 44 mille 214 dollars.

Il ajoute que ce taux place Israël au premier rang mondial dans le domaine de la recherche et du développement, et au cinquième dans les technologies modernes (compte tenu de la population), tandis que la part des exportations israéliennes dans le domaine de la haute technologie a atteint environ 54% en 2021.

Quant à la part des employés dans le secteur de la haute technologie, elle s'élève à 10,4 % de la main-d'œuvre totale en 2021.

Afin de développer le centre de Beer-Sheva, la Direction du cyberespace d'Israël apporte son soutien aux entreprises qui s'installent dans la région.

Depuis la même ville, le centre de gestion des cyber-incidents gère le projet "Dôme de fer", qui vise en général à surveiller et à suivre diverses cyberattaques ciblant toutes les infrastructures en Israël.

Dans une déclaration à la MAP, le directeur exécutif de la politique et de la stratégie au département israélien de la cybersécurité, Roy Yarom a indiqué que le projet "Dôme de fer" fournira une protection complète des installations économiques et administratives, ainsi que des PC à même d'améliorer la défense du cyberespace israélien et renforcer sa structure de bouclier.

M. Yarom souligne, en outre, qu'Internet deviendra inévitablement l'une des dimensions de la guerre future, sinon la plus importante.

Il dit également que tout le monde devrait prendre la cybersécurité au sérieux car les cybercriminels ciblent non seulement les agences gouvernementales et les institutions privées, mais aussi les employés, les gens ordinaires et même les enfants et les mineurs, les catégories les plus vulnérables de la société.

D'autre part, il a mis en avant qu'il existe des opportunités prometteuses de coopération entre le Maroc et Israël dans le domaine de la cybersécurité et du numérique pour un cyberespace ouvert, fiable, sécurisé et stable.

M. Yarom a mis en exergue les opportunités prometteuses de coopération dans les domaines académique et scientifique, la recherche et le développement, en plus de l'échange d'informations et de compétences, d'étudiants et l'organisation de recherches conjointes.

Il a également souligné l'importance d'améliorer ces échanges, afin de répondre aux menaces mondiales et d'asseoir des normes de comportement responsable dans le cyberespace.

Au vu du développement important du secteur de la cybersécurité en Israël, du nombre de transactions qu'il réalise et de l'attractivité croissante qu'il connait à l'échelle mondiale, un rendez-vous international annuel régulier est organisé sous le nom de "Cyber Week", dont la dernière édition a été tenue à l'Université de Tel-Aviv en juin dernier, en coopération avec le ministère israélien des Affaires étrangères.

Cet événement international offre aux experts de l'industrie, du gouvernement, de la défense et du milieu universitaire l'occasion de partager leurs connaissances sur les défis et les opportunités dans ce domaine, de discuter des questions des cyberattaques, des dommages causés aux infrastructures vitales des pays, des dépenses publiques dédiées au secteur de l'informatique, des dépenses allouées à la cyber-protection et de la violation de la vie privée.

Selon les résultats de l'une des études présentées lors de la dernière édition de cette conférence, les dépenses de cybersécurité destinées à la protection des données et à la gestion des risques liés à l'informatique devraient atteindre 172 milliards de dollars dans le monde en 2022.

Une autre étude a rapporté que la cybercriminalité a considérablement augmenté pendant la pandémie de Covid-19, la fraude en ligne s'est accrue de plus de 400% en 2020 par rapport aux années précédentes et les messages frauduleux ont doublé de façon spectaculaire alors que Google a bloqué quotidiennement plus de 18 millions d'e-mails malveillants et d'hameçonnage durant la pandémie.

Cela comprend les escroqueries, le vol ainsi que l'implantation de logiciels de suivi malveillants et d'espionnage.

وكالة المغرب العربي للأنباء
MAP
AGENCE MAROCAINE DE PRESSE
The value of information

Ciberseguridad: Un interés global creciente frente a un aumento de los ciberataques

Tel Aviv - Por Abderrazak Trebak La necesidad de la ciberseguridad para proteger sistemas, redes y datos está aumentando en todo el mundo, con la aceleración de la transformación digital de las sociedades y diversas actividades económicas y sociales, así como los riesgos de un aumento de los ataques cibernéticos, el fraude y la piratería.

Estudios recientes registran un alarmante aumento de la guerra y los delitos cibernéticos, y estiman que los daños asociados a estas amenazas alcanzan los 10,5 billones de dólares anuales para 2025 en todo el mundo.

Esos ciberataques suelen tener por objeto el acceso a información delicada para robar o destruir, interrumpir redes u obtener fondos, lo que requiere una gran demanda por parte de los gobiernos y las empresas de soluciones cibernéticas para proteger la infraestructura, los equipamientos, las instalaciones y diversos sistemas económicos, financieros y otros.

"Los gobiernos deben gastar más para proteger las redes y los sistemas de información, e invertir en investigación cibercientífica y en tripulaciones humanas para usar estas herramientas eficientemente", dijo Ran Natanzon, director del Departamento de Sistemas de Información e Innovación del Ministerio de Asuntos Exteriores israelí, en una declaración a la MAP, al margen de la visita de una delegación de periodistas internacionales a Tel Aviv.

En Israel, los datos de la industria de la seguridad cibernética muestran que en 2021 se logró un número récord de transacciones de 8,8 mil millones de dólares.

El general mayor, el matemático Isaac Ben-Israel, conocido como el padre del programa de la ciberindustria israelí, subrayó, en su reunión con la delegación de periodistas internacionales, que "al usar Internet, todos están expuestos, los datos son visibles para muchos, el dinero está expuesto, la vida personal, la salud y la seguridad, así como las actividades de los departamentos gubernamentales".

Y añadió que Israel se ha fijado como objetivo ser "una de las cinco mayores potencias del mundo en el ámbito de la ciberindustria y su consolidación como fuerza electrónica, así que hemos creado un centro de investigación electrónica en cada universidad, y hoy impartimos clases de ciberseguridad en las escuelas secundarias".

Este gran interés por el sector cibernético se refleja en el notable desarrollo conocido por el nuevo polo tecnológico en la ciudad de Beerseba, en el desierto del Néguev, que actualmente incluye a más de 70 grandes empresas que emplean aproximadamente a 2.500 personas, la mayoría de las cuales son ingenieros de información.

El plan estratégico para los próximos años estipula que este polo estará compuesto por 15 edificios inteligentes que ofrecen 10.000 empleos en inteligencia artificial e ingeniería, centros de investigación innovadores para alarma y respuesta a ataques informáticos, algunos de los cuales están supervisados por equipos especializados del ejército.

Dentro de este polo en la ciudad de Beerseba, hay unidades electrónicas pertenecientes al ejército, y las principales empresas israelíes en el sector, especialmente las compañías de programación CheckPoint, Nir Zuk's Palo Alto Networks, SentinelOne y Cybereason, así como centros para grandes empresas internacionales como Google, Intel, Microsoft y otros.

El centro de Beerseba complementará otros centros en Tel Aviv y Haifa y tiene como objetivo hacer de Israel uno de los mejores cibercentros del mundo, agregó Ran Natanzon.

También señaló que esta tendencia fortalecería el sector de la investigación científica y el desarrollo, que en Israel representa el 4,5% del producto interno bruto (2021), teniendo en cuenta que el producto interno bruto (PIB) per cápita alcanzó los 44.214 dólares en el cuarto trimestre de 2021.

El mismo agregó que este promedio convierte a Israel en líder mundial en materia de densidad de la investigación científica e innovación, y la quinta a nivel mundial en la densidad de las nuevas tecnologías (en comparación con el número de habitantes). En cuanto a las exportaciones israelíes en el ámbito de las tecnologías punteras alcanzó el 54% en 2021, mientras que el promedio de los empleados en el dominio de las altas tecnologías se situó en el 10,4% del total de la mano de obra en 2021.

Con el fin de desarrollar el centro de Beerseba, la Dirección Israelí para el Espacio Electrónico ofrece apoyo a las empresas que se trasladan a esta región.

En la misma ciudad, el Centro de Gestión de Eventos Cibernéticos gestiona el proyecto del "Domo de Hierro en la Defensa Cibernética" que identifica y sigue los diferentes ataques cibernéticos dirigidos contra las diferentes infraestructuras en Israel.

En una declaración a la MAP, Roy Yarom, director ejecutivo para política y estrategia en la Dirección Israelí de Seguridad Cibernética, indicó que "el Domo de Hierra en la Defensa Cibernética" garantizará una protección completa para las instalaciones económicas y administrativas e incluso para los ordenadores personales, lo que consolidará la protección del espacio electrónico israelí y reforzará su estructura en la defensa y el enfrentamiento.

Según Yarom, que asegura que internet será sin duda una, o la más importante, dimensión de las guerras del futuro, todo el mundo tiene que tomar con seriedad la seguridad cibernética, puesto que los criminales cibernéticos no atacan solamente las agencias gubernamentales y las instituciones privadas, sino también a los funcionarios y las personas de a pie, e incluso a los niños y los menores, que son las categorías más vulnerables de la sociedad.

Por otra parte, destacó que hay una oportunidad prometedora de cooperación entre Marruecos e Israel en el ámbito cibernético y la tecnología digital a favor de un espacio electrónico abierto, seguro y estable.

Asimismo, Yarom puso de relieve las oportunidades prometedoras de cooperación en los dominios universitario y científico y de la investigación y el desarrollo, además del intercambio de informaciones y experiencias, y el intercambio de estudiantes y la organización de investigaciones conjuntas.

En la misma línea, subrayó la importancia de consolidar el intercambio de informaciones para hacer frente a las amenazas globales comunes y aplicar las medidas del comportamiento responsable en el espacio cibernético.

Vista la importante evolución que experimenta el ámbito de la seguridad cibernética en Israel, el volumen de negocios que registra y la atracción creciente que conoce a nivel mundial, se organiza un encuentro anual regular bautizado "Semana Cibernética", cuya última edición tuvo lugar, el 30 de junio, en la Universidad de Tel-Aviv, en cooperación con el ministerio israelí de Asuntos Exteriores.

La "Semana Cibernética" es un evento internacional que ofrece a los expertos de la industria, los gobiernos, la defensa y los círculos académicos, la oportunidad de compartir sus conocimientos sobre los desafíos y las oportunidades en este ámbito, además de examinar las cuestiones de los ataques electrónicos y los daños a la infraestructura vital de los Estados, y la financiación pública sobre la tecnología de la información y el ritmo de la financiación de la seguridad electrónica y la violación de la privacidad.

Según un estudio que fue presentado durante la última edición de este encuentro, se prevé que la financiación de la seguridad cibernética dirigida a la protección de datos y la gestión de riesgos digitales alcance los 172 mil millones de dólares a nivel mundial en 2022.

Otro estudio afirma que el cibercrimen creció considerablemente durante la pandemia de Covid-19, mientras que las operaciones de fraude a través de internet subieron más de 400% en 2020 en comparación con los años anteriores. Igualmente, los mensajes fraudulentos se multiplicaron notablemente, hasta el punto de que Google tuvo que prohibir cada día, durante la pandemia, 18 millones de mensajes electrónicos maliciosos y fraudulentos. Estos mensajes incluyen el fraude, el robo y la implantación de programas dañinos de localización y espionaje.

الأمن السيبراني .. اهتمام عالمي في ارتفاع مع توالي وتيرة الهجمات الإلكترونية

عبد الرزاق طريبق

تل أبيب ـــ تتزايد عبر العالم الحاجة الى الأمن السيبراني لحماية الأنظمة والشبكات والبيانات، مع تسارع وتيرة التحول الرقمي للمجتمعات ومختلف الأنشطة الاقتصادية والاجتماعية، وما يكتنف ذلك أيضا من مخاطر ارتفاع وتيرة الهجمات الإلكترونية وعمليات الاحتيال والقرصنة.

وتسجل دراسات حديثة ارتفاعا مثيرا للقلق في الحرب والجرائم الإلكترونية، وتقدر أن يصل الضرر المرتبط بذلك إلى ١٠,٥ تريليون دولار سنويا بحلول عام ٢٠٢٥ على الصعيد العالمي.

وغالبا ما تهدف هذه الهجمات الإليكترونية إلى الوصول إلى المعلومات الحساسة لسرقتها أو تدميرها وتعطيل الشبكات أو الحصول على الأموال، ويفرض ذلك ارتفاع طلب الحكومات والشركات على الحلول السيبرانية، لحماية البنيات

ويقول Ran Natanzon ران ناتازون مدير إدارة أنظمة المعلومات والابتكار بوزارة الخارجية الإسرائيلية في تصريح لوكالة المغرب العربي الأنباء، على هامش زيارة لوفد من الصحافيين الدوليين لتل أبيب، إن "الحكومات مطالبة بالمزيد من الإنفاق لحماية الشبكات والأنظمة المعلوماتية، والاستثمار في البحث العلمي السيبراني وفي الأطقم البشرية من أجل استخدام هذه الأدوات بكفاءة".

وفي إسرائيل تظهر بيانات صناعة الأمن السيبراني أنه في عام ٢٠٢١ تم تحقيق رقم معاملات وصل الى مستوى قياسي بلغ ٨,٨ مليار دولار.

ويقول الجنرال ماجور عالم الرياضيات إسحاق بن إسرائيل، المعروف بكونه أب برنامج الصناعة السيبرانية الإسرائيلي، في لقائه مع وفد الصحافيين الدوليين "باستعمال الانترنت يصبح الكل مكشوفا، فالبيانات تكون مرئية للكثيرين والأموال مكشوفة وكذلك الحياة الشخصية، والصحة والأمن علاوة على أنشطة الإدارات الحكومية".

ويضيف أن إسرائيل وضعت لنفسها أن تكون "من بين خمسة قوى كبرى في العالم في مجال الصناعة السيبرانية وترسيخ نفسها كقوة إلكترونية، ولذلك قمنا بإنشاء مركز أبحاث إلكتروني في كل جامعة، واليوم أصبحنا ندرس الأمن السيبراني في المدارس الثانوية".

التحتية والتجهيزات والمنشآت ومختلف الأنظمة الاقتصادية والمالية وغيرها.

هذا الاهتمام البالغ بالقطاع السيبراني يتجلي بوضوح في التطور الملفت الذي يعرفه القطب التكنولوجي الجديد بمدينة بئر السبع في صحراء النقب، والذي يضم حاليا أزيد من ٧٠ من كبريات الشركات التي توظف ما يقرب من ٢٥٠٠ شخص معظمهم مهندسو معلوميات.

يقول Ran Natanzon ران ناتازون إن الخطة الاستراتيجية للسنوات المقبلة تتوقع أن يتشكل هذا القطب من ١٥ مبنى ذكيا، يوفر عشرة آلاف وظيفة في الذكاء الاصطناعي والهندسة المعلوماتية، ومراكز جد متطورة للبحث والابتكار وللإنذار والاستجابة لهجمات الكمبيوتر، بعضها تشرف عليه فرق متخصصة من الجيش.

وضمن هذا القطب بمدينة بئر السبع تتواجد الوحدات الإلكترونية التابعة للجيش، والشركات الإسرائيلية الكبرى في المجال، خصوصا شركات البرمجيات CheckPoint و Nir Zuk's Palo Alto Networks و SentinelOne و Cybereason، علاوة على مراكز لكبريات الشركات العالمية مثل غوغل وأنتيل وميكروسوفت وغيرها.

ويضيف ران ناتازون إن مركز بئر السبع سيكون مكملا للمراكز الأخرى المتواجدة في تل أبيب وحيفا والذي يهدف

كما أشار الى أن هذا التوجه سيعزز قوة قطاع البحث العلمي والتطوير والذي يمثل في إسرائيل ٥ر٤ في المائة من الناتج الداخلي الخام (٢٠٢١) علما أن حصة الفرد في الناتج الداخلي الخام بلغت في الربع الرابع من ٢٠٢١ نحو ٤٤ الف و٢١٤ دولار.

ويضيف أن هذا المعدل يجعل إسرائيل تحتل الرتبة الأولى عالميا في مجال كثافة البحث العلمي والتطوير، والخامسة عالميا في كثافة التكنولوجيات الحديثة high tech density (بالنظر لعدد السكان)، فيما بلغت حصة الصادرات الإسرائيلية في مجال التكنولوجيات الدقيقة high tech نحو ٥٤ في المائة في عام ٢٠٢١، أما نسبة العاملين في قطاع التكنولوجيا العالية فقد بلغت ٤ر١٠ في المائة في مجموع القوة العاملة في عام ٢٠٢١.

ومن أجل تطوير مركز بئر السبع، تقدم المديرية الإسرائيلية للفضاء الإلكتروني دعما للشركات التي تنتقل إلى المنطقة.

ومن المدينة ذاتها يدير مركز إدارة الأحداث السيبرانية مشروع "القبة الحديدية في الدفاع السيبراني" والذي يعمل على رصد ونتبع مختلف الهجمات السيبيرانية التي تستهدف جميع مرافق البنية التحتية في إسرائيل بشكل كامل.

يقول روم ياروم Roy yarom المدير التنفيذي للسياسة والاستراتيجية بالإدارة الإسرائيلية للأمن السيبراني، في تصريح لوكالة المغرب العربي للأنباء إن مشروع "القبة الحديدية في الدفاع السيبراني" سيقدم حماية شاملة للمرافق الاقتصادية والإدارية وحتى للحواسيب الشخصية، بما يعزز الدفاع عن الفضاء الإلكتروني الإسرائيلي وتقوية بنيته في الدرع والمواجهة.

ويؤكد روم ياروم أن الإنترنت سيصبح حتما أحد أبعاد الحرب المستقبلية، إن لم يكن أهمها.

ويقول إنه يتعين أن يأخذ الجميع الأمن السيبراني على محمل الجد لأن مجرمي الإنترنت لا يستهدفون الوكالات الحكومية والمؤسسات الخاصة فقط، بل أيضا الموظفين والأشخاص العاديين وحتى الأطفال والقاصرين لأنهم أكثر قطاعات المجتمع ضعفا.

الأمن السيبراني .. اهتمام عالمي في ارتفاع مع توالي وتيرة الهجمات الإلكترونية

تل أبيب ـــ تتزايد عبر العالم الحاجة الى الأمن السيبراني لحماية الأنظمة والشبكات والبيانات، مع تسارع وتيرة التحول الرقمي للمجتمعات ومختلف الأنشطة الاقتصادية والاجتماعية، وما يكتنف ذلك أيضا من مخاطر ارتفاع وتيرة الهجمات الإلكترونية وعمليات الاحتيال والقرصنة.

وتسجل دراسات حديثة ارتفاعا مثيرا للقلق في الحرب والجرائم الإلكترونية، وتقدر أن يصل الضرر المرتبط بذلك إلى ١٠,٥ تريليون دولار سنويا بحلول عام ٢٠٢٥ على الصعيد العالمي.

وغالبا ما تهدف هذه الهجمات الإليكترونية إلى الوصول إلى المعلومات الحساسة لسرقتها أو تدميرها وتعطيل الشبكات أو الحصول على الأموال، ويفرض ذلك ارتفاع طلب الحكومات والشركات على الحلول السيبرانية، لحماية البنيات التحتية والتجهيزات والمنشآت ومختلف الأنظمة الاقتصادية والمالية وغيرها.

ويقول Ran Natanzon ران ناتازون مدير إدارة أنظمة المعلومات والابتكار بوزارة الخارجية الإسرائيلية في تصريح لوكالة المغرب العربي الأنباء، على هامش زيارة لوفد من الصحافيين الدوليين لتل أبيب، إن "الحكومات مطالبة بالمزيد من الإنفاق لحماية الشبكات والأنظمة المعلوماتية، والاستثمار في البحث العلمي السيبراني وفي الأطقم البشرية من أجل استخدام هذه الأدوات بكفاءة".

وفي إسرائيل تظهر بيانات صناعة الأمن السيبراني أنه في عام ٢٠٢١ تم تحقيق رقم معاملات وصل الى مستوى قياسي بلغ ٨,٨ مليار دولار.

ويقول الجنرال ماجور عالم الرياضيات إسحاق بن إسرائيل، المعروف بكونه أب برنامج الصناعة السيبرانية الإسرائيلي، في لقائه مع وفد الصحافيين الدوليين "باستعمال الانترنت يصبح الكل مكشوفا، فالبيانات تكون مرئية للكثيرين والأموال مكشوفة وكذلك الحياة الشخصية، والصحة والأمن علاوة على أنشطة الإدارات الحكومية".

ويضيف أن إسرائيل وضعت لنفسها أن تكون "من بين خمسة قوى كبرى في العالم في مجال الصناعة السيبرانية وترسيخ نفسها كقوة إلكترونية، ولذلك قمنا بإنشاء مركز أبحاث إلكتروني في كل جامعة، واليوم أصبحنا ندرس الأمن السيبراني في المدارس الثانوية".

وأشار من جهة أخرى الى أن ثمة فرصا واعدة للتعاون بين المغرب وإسرائيل في المجال السيبراني والتكنولوجيا الرقمية من أجل فضاء إلكتروني مفتوح وموثوق وآمن ومستقر.

لجعل إسرائيل واحدا من أكبر المراكز العالمية في المجال السيبيراني.

وأبرز ياروم الفرص الواعدة للتعاون في المجال الجامعي والعلمي والبحث والتطوير، بالإضافة إلى تبادل المعلومات والمهارات، وتبادل الطلبة وتنظيم أبحاث مشتركة.

كما أكد أهمية تعزيز تبادل المعلومات من أجل الاستجابة للتهديدات الشاملة المشتركة، وتنفيذ معايير السلوك المسؤول في الفضاء السيبراني.

وبالنظر للتطور الهام الذي يعرفه قطاع الأمن السيبراني في إسرائيل، ورقم المعاملات الذي يحققه والاستقطاب المتزايد الذي يشهده عالميا أصبح يخصص له لقاء سنوي دولي منتظم تحت مسمى "الأسبوع السيبيراني" احتضنت دورته الأخيرة في ٣٠ يونيو الماضي جامعة تل أبيب بتعاون مع وزارة الخارجية الإسرائيلية.

ويعتبر هذا الأسبوع حدثا دوليا يوفر فرصة للخبراء من الصناعة والحكومات والدفاع والأوساط الأكاديمية لمشاركة معرفتهم حول التحديات والفرص في هذا المجال، ومناقشة قضايا الهجمات الإلكترونية والأضرار بالبنية التحتية الحيوية للدول، والإنفاق العام على تكنولوجيا المعلومات، ووتيرة الإنفاق على الحماية الإلكترونية، وانتهاك الخصوصية.

وبحسب نتائج إحدى الدراسات التي عرضت خلال الدورة الأخيرة من هذا المؤتمر فمن المتوقع أن يصل الإنفاق على الأمن السيبراني الموجه لحماية البيانات وإدارة المخاطر المعلوماتية إلى ١٧٢ مليار دولار على مستوى العالم في عام ٢٠٢٢.

وأفادت دراسة أخرى أن الجريمة السيبرانية ارتفعت بشكل كبير خلال جائحة كوفيد ١٩، وتزايدت عمليات الاحتيال عبر الإنترنت بأكثر من ٤٠٠ فى المائة في عام ٢٠٢٠ مقارنة بالسنوات السابقة، كما تضاعفت الرسائل الاحتيالية بشكل كبير حيث قامت غوغل بحظر أكثر من ١٨ مليون رسالة بريد إلكتروني ضارة وتصيد احتيالي يوميا خلال الجائحة، ويشمل ذلك رسائل الاحتيال والسرقة وأيضا زرع برامج خبيثة للتعقب والتجسس .

هذا الاهتمام البالغ بالقطاع السيبراني يتجلي بوضوح في التطور الملفت الذي يعرفه القطب التكنولوجي الجديد بمدينة بئر السبع في صحراء النقب، والذي يضم حاليا أزيد من ٧٠ من كبريات الشركات التي توظف ما يقرب من ٢٥٠٠ شخص معظمهم مهندسو معلوميات.

يقول Ran Natanzon ران ناتازون إن الخطة الاستراتيجية للسنوات المقبلة تتوقع أن يتشكل هذا القطب من ١٥ مبنى ذكيا، يوفر عشرة آلاف وظيفة في الذكاء الاصطناعي والهندسة المعلوماتية، ومراكز جد متطورة للبحث والابتكار وللإنذار والاستجابة لهجمات الكمبيوتر، بعضها تشرف عليه فرق متخصصة من الجيش.

وضمن هذا القطب بمدينة بئر السبع تتواجد الوحدات الإلكترونية التابعة للجيش، والشركات الإسرائيلية الكبرى في المجال، خصوصا شركات البرمجيات CheckPoint و Nir Zuk's Palo Alto Networks و SentinelOne و Cybereason، علاوة على مراكز لكبريات الشركات العالمية مثل غوغل وأنتيل وميكروسوفت وغيرها.

ويضيف ران ناتازون إن مركز بئر السبع سيكون مكملا للمراكز الأخرى المتواجدة في تل أبيب وحيفا والذي يهدف لجعل إسرائيل واحدا من أكبر المراكز العالمية في المجال السيبيراني.

كما أشار الى أن هذا التوجه سيعزز قوة قطاع البحث العلمي والتطوير والذي يمثل في إسرائيل ٤ر٥ في المائة من الناتج الداخلي الخام (٢٠٢١) علما أن حصة الفرد في الناتج الداخلي الخام بلغت في الربع الرابع من ٢٠٢١ نحو ٤٤ الف و٢١٤ دولار.

ويضيف أن هذا المعدل يجعل إسرائيل تحتل الرتبة الأولى عالميا في مجال كثافة البحث العلمي والتطوير، والخامسة عالميا في كثافة التكنولوجيات الحديثة high tech density (بالنظر لعدد السكان)، فيما بلغت حصة الصادرات الإسرائيلية في مجال التكنولوجيات الدقيقة high tech نحو ٥٤ في المائة في عام ٢٠٢١، أما نسبة العاملين في قطاع التكنولوجيا العالية فقد بلغت ٤ر١٠ في المائة في مجموع القوة العاملة في عام ٢٠٢١.

ومن أجل تطوير مركز بئر السبع، تقدم المديرية الإسرائيلية للفضاء الإلكتروني دعما للشركات التي تنتقل إلى المنطقة.

ومن المدينة ذاتها يدير مركز إدارة الأحداث السيبرانية مشروع "القبة الحديدية في الدفاع السيبراني" والذي يعمل على رصد وتتبع مختلف الهجمات السيبيرانية التي تستهدف جميع مرافق البنية التحتية في إسرائيل بشكل كامل.

يقول روم ياروم Roy yarom المدير التنفيذي للسياسة والاستراتيجية بالإدارة الإسرائيلية للأمن السيبراني، في تصريح لوكالة المغرب العربي للأنباء إن مشروع "القبة الحديدية في الدفاع السيبراني" سيقدم حماية شاملة للمرافق الاقتصادية والإدارية وحتى للحواسيب الشخصية، بما يعزز الدفاع عن الفضاء الإلكتروني الإسرائيلي وتقوية بنيته في الدرع والمواجهة.

ويؤكد روم ياروم أن الإنترنت سيصبح حتما أحد أبعاد الحرب المستقبلية، إن لم يكن أهمها.

ويقول إنه يتعين أن يأخذ الجميع الأمن السيبراني على محمل الجد لأن مجرمي الإنترنت لا يستهدفون الوكالات الحكومية والمؤسسات الخاصة فقط، بل أيضا الموظفين والأشخاص العاديين وحتى الأطفال والقاصرين لأنهم أكثر قطاعات المجتمع ضعفا.

وأشار من جهة أخرى الى أن ثمة فرصا واعدة للتعاون بين المغرب وإسرائيل في المجال السيبراني والتكنولوجيا الرقمية من أجل فضاء إلكتروني مفتوح وموثوق وآمن ومستقر.

وأبرز ياروم الفرص الواعدة للتعاون في المجال الجامعي والعلمي والبحث والتطوير، بالإضافة إلى تبادل المعلومات والمهارات، وتبادل الطلبة وتنظيم أبحاث مشتركة.

كما أكد أهمية تعزيز تبادل المعلومات من أجل الاستجابة للتهديدات الشاملة المشتركة، وتنفيذ معايير السلوك المسؤول في الفضاء السيبراني.

وبالنظر للتطور الهام الذي يعرفه قطاع الأمن السيبراني في إسرائيل، ورقم المعاملات الذي يحققه والاستقطاب المتزايد الذي يشهده عالميا أصبح يخصص له لقاء سنوي دولي منتظم تحت مسمى "الأسبوع السيبيراني" احتضنت دورته الأخيرة في ٣٠ يونيو الماضي جامعة تل أبيب بتعاون مع وزارة الخارجية الإسرائيلية.

ويعتبر هذا الأسبوع حدثا دوليا يوفر فرصة للخبراء من الصناعة والحكومات والدفاع والأوساط الأكاديمية لمشاركة معرفتهم حول التحديات والفرص في هذا المجال، ومناقشة قضايا الهجمات الإلكترونية والأضرار بالبنية التحتية الحيوية للدول، والإنفاق العام على تكنولوجيا المعلومات، ووتيرة الإنفاق على الحماية الإلكترونية، وانتهاك الخصوصية.

وبحسب نتائج إحدى الدراسات التي عرضت خلال الدورة الأخيرة من هذا المؤتمر فمن المتوقع أن يصل الإنفاق على الأمن السيبراني الموجه لحماية البيانات وإدارة المخاطر المعلوماتية إلى ١٧٣ مليار دولار على مستوى العالم في عام ٢٠٢٢.

وأفادت دراسة أخرى أن الجريمة السيبرانية ارتفعت بشكل كبير خلال جائحة كوفيد ١٩، وتزايدت عمليات الاحتيال عبر الإنترنت بأكثر من ٤٠٠ فى المائة في عام ٢٠٢٠ مقارنة بالسنوات السابقة، كما تضاعفت الرسائل الاحتيالية بشكل كبير حيث قامت غوغل بحظر أكثر من ١٨ مليون رسالة بريد إلكتروني ضارة وتصيد احتيالي يوميا خلال الجائحة، ويشمل ذلك رسائل الاحتيال والسرقة وأيضا زرع برامج خبيثة للتعقب والتجسس .

NEWS AFRICA Premier African News Portal NOW

Cyber Security: Global Attention on the Rise as Cyber Attacks Escalate

The need for cybersecurity to protect systems, networks and data is increasing worldwide, with the accelerating digital transformation of societies and various economic and social activities, as well as the risks of mass cyber attacks, fraud and hacking.

Recent studies reveal an alarming rise in war and cybercrime, and estimate that the associated damage will reach $10.5 trillion annually by 2025 globally.

Cyber attacks are often aimed at accessing sensitive information to steal or destroy it, disrupt networks or obtain funds.

Faced with this situation, governments and companies are opting for cybersecurity solutions to protect infrastructure, equipment, facilities, and various economic and financial systems.

"Governments are required to work more to protect networks and information systems, and to invest in cyber scientific research and human capital in order to efficiently use these tools," Ran Natanzon, Head of innovation & Country branding, Public Diplomacy Division at Ministry of Foreign Affairs of Israel, told MAP on the sidelines of a visit of a delegation of international journalists to Tel Aviv.

In Israel, cyber industry data show that in 2021, a significant number of transactions were made, reaching a record level of $8.8 billion.

For his part, Major General and mathematician Issac Ben-Israel, a pioneer in Israel's cyber-industry program, said that "with the use of the Internet, 'everything becomes exposed'. Data is visible, and funds are discovered, as well as privacy, health and security, in addition to the activities of government administrations".

He added that Israel sets itself to be "among the five major powers in the world in the field of cyberindustry and stands out as an electronic force, and that is why we have established an electronic research center in every university, and today we teach cybersecurity in secondary schools."

This interest in the cyber sector is most evident in the remarkable development of the new technological pole in the city of Beersheba in the Negev desert, which currently hosts more than 70 of the largest companies employing nearly 2,500 people, most of whom are information engineers.

Ran Natanzon indicated that the strategic plan for the coming years foresees that this center will include 15 intelligent buildings, providing about ten thousand jobs in artificial intelligence and computer engineering, and highly developed centers for research, innovation, alert and response to computer attacks, some of which will be under the supervision of specialized teams from the army.

This pole in the city of Beersheba also houses the electronic units of the army and the major Israeli companies in the field, especially the software companies CheckPoint, Nir Zuk's Palo Alto Networks, SentinelOne and Cybereason, in addition to centers of the largest international companies such as Google, Intel, and Microsoft, among others.

Ran Natason pointed out that the Beersheba center complements the others in Tel Aviv and Haifa, which aim to make Israel one of the world's leading countries in the field of cybersecurity.

He also stressed that this trend will strengthen the scientific research and development sector, which in Israel represents 5.4% of the gross domestic product (GDP) (2021), given the fact that the per capita GDP amounted to 44,214 dollars in the fourth quarter of 2021.

This rate places Israel at the top world rank in terms of scientific research and development intensity, and at the fifth world rank in modern technology density (per population), while the share of Israeli exports in the high-tech sector has reached about 54 percent in 2021.

As for the percentage of workers in the high-tech sector, it reached 10.4 percent of the total workforce in 2021.

To develop the Beersheba Center, Israel's Cyberspace Directorate provides support to companies that set up shop in the area.

From the same city, the National Cyber Directorate manages the "Iron Dome in Cyber Defense" project, which aims to monitor and track various cyber attacks that target all infrastructure in Israel.

In a statement to MAP, Roy Yarom, executive director of policy and strategy at the Israeli Department of Cybersecurity, said that the "Iron Dome in Cyber Defense" project will provide comprehensive protection of economic and administrative facilities, and even personal computers, in a way that enhances the defense of Israeli cyberspace and strengthens its structure in both shielding and confrontation.

Rom Yarom pointed out that the Internet will inevitably become one of the dimensions of future warfare, if not the most important.

He said that everyone should take cybersecurity seriously because cybercriminals target not only government agencies and private institutions, but also employees, ordinary people, and even children and minors because they are the most vulnerable sectors of society.

On the other hand, he stressed that there are promising opportunities for cooperation between Morocco and Israel in the cyber and digital field for open, reliable, secure, and stable cyberspace.

Yarom highlighted the promising opportunities for cooperation in the academic and scientific fields, research, and development, in addition to exchanging information and skills, as well as students and organizing joint research.

He stressed the importance of promoting information exchange to respond to common cross-cutting threats and to implement standards of responsible behavior in cyberspace.

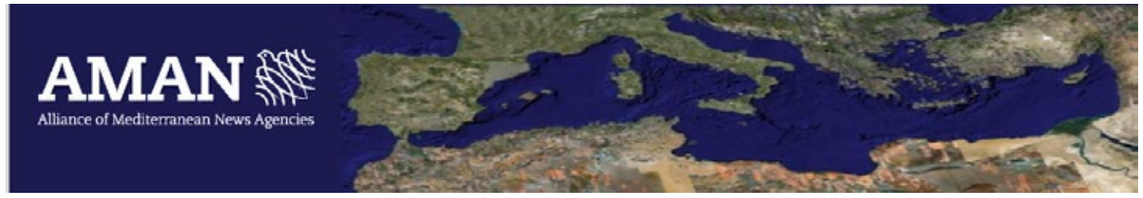
In view of the significant development of the cybersecurity sector in Israel, the number of transactions it carries out and its growing attractiveness on a global scale, a regular annual international event is organized under the name of "Cyber Week", the latest edition of which was held at Tel Aviv University last June, in cooperation with the Israeli Ministry of Foreign Affairs.

The week is an international event that provides an opportunity for experts from industry, government, defense, and academia to share their knowledge on challenges and opportunities in the field, and to discuss cyberattacks, damage to countries' critical infrastructure, public spending on information technology, the pace of spending on cyber protection, and privacy infringement.

According to the results of a study presented at the last session of the conference, spending on cybersecurity for data protection and information risk management is expected to reach $172 billion worldwide in 2022.

Another study reported that cybercrime increased significantly during the Covid 19 pandemic, and online fraud increased by more than 400% in 2020 compared to previous years, and fraudulent messages dramatically doubled as Google blocked more than 18 million malicious and phishing emails during the pandemic.

This includes scams, theft as well as the implementation of malicious tracking and spyware.



MAP - Cyber Security: Global Attention on the Rise as Cyber Attacks Escalate

By Abderrazak Trebak -Tel Aviv -July 22,2022-(MAP)- The need for cybersecurity to protect systems, networks and data is increasing worldwide, with the accelerating digital transformation of societies and various economic and social activities, as well as the risks of mass cyber attacks, fraud and hacking.

Recent studies reveal an alarming rise in war and cybercrime, and estimate that the associated damage will reach $10.5 trillion annually by 2025 globally.

Cyber attacks are often aimed at accessing sensitive information to steal or destroy it, disrupt networks or obtain funds.

Faced with this situation, governments and companies are opting for cybersecurity solutions to protect infrastructure, equipment, facilities, and various economic and financial systems.

"Governments are required to work more to protect networks and information systems, and to invest in cyber scientific research and human capital in order to efficiently use these tools," Ran Natanzon, Head of innovation & Country branding, Public Diplomacy Division at Ministry of Foreign Affairs of Israel, told MAP on the sidelines of a visit of a delegation of international journalists to Tel Aviv.

In Israel, cyber industry data show that in 2021, a significant number of transactions were made, reaching a record level of $8.8 billion.

For his part, Major General and mathematician Issac Ben-Israel, a pioneer in Israel's cyber-industry program, said that "with the use of the Internet, 'everything becomes exposed'. Data is visible, and funds are discovered, as well as privacy, health and security, in addition to the activities of government administrations".

He added that Israel sets itself to be "among the five major powers in the world in the field of cyberindustry and stands out as an electronic force, and that is why we have established an electronic research center in every university, and today we teach cybersecurity in secondary schools."

This interest in the cyber sector is most evident in the remarkable development of the new technological pole in the city of Beersheba in the Negev desert, which currently hosts more than 70 of the largest companies employing nearly 2,500 people, most of whom are information engineers.

Ran Natanzon indicated that the strategic plan for the coming years foresees that this center will include 15 intelligent buildings, providing about ten thousand jobs in artificial intelligence and computer engineering, and highly developed centers for research, innovation, alert and response to computer attacks, some of which will be under the supervision of specialized teams from the army.

This pole in the city of Beersheba also houses the electronic units of the army and the major Israeli companies in the field, especially the software companies CheckPoint, Nir Zuk's Palo Alto Networks, SentinelOne and Cybereason, in addition to centers of the largest international companies such as Google, Intel, and Microsoft, among others.

Ran Natason pointed out that the Beersheba center complements the others in Tel Aviv and Haifa, which aim to make Israel one of the world's leading countries in the field of cybersecurity.

He also stressed that this trend will strengthen the scientific research and development sector, which in Israel represents 5.4% of the gross domestic product (GDP) (2021), given the fact that the per capita GDP amounted to 44,214 dollars in the fourth quarter of 2021.

This rate places Israel at the top world rank in terms of scientific research and development intensity, and at the fifth world rank in modern technology density (per population), while the share of Israeli exports in the high-tech sector has reached about 54 percent in 2021.

As for the percentage of workers in the high-tech sector, it reached 10.4 percent of the total workforce in 2021.

To develop the Beersheba Center, Israel's Cyberspace Directorate provides support to companies that set up shop in the area.

From the same city, the National Cyber Directorate manages the "Iron Dome in Cyber Defense" project, which aims to monitor and track various cyber attacks that target all infrastructure in Israel.

In a statement to MAP, Roy Yarom, executive director of policy and strategy at the Israeli Department of Cybersecurity, said that the "Iron Dome in Cyber Defense" project will provide comprehensive protection of economic and administrative facilities, and even personal computers, in a way that enhances the defense of Israeli cyberspace and strengthens its structure in both shielding and confrontation.

Rom Yarom pointed out that the Internet will inevitably become one of the dimensions of future warfare, if not the most important.

He said that everyone should take cybersecurity seriously because cybercriminals target not only government agencies and private institutions, but also employees, ordinary people, and even children and minors because they are the most vulnerable sectors of society.

On the other hand, he stressed that there are promising opportunities for cooperation between Morocco and Israel in the cyber and digital field for open, reliable, secure, and stable cyberspace.

Yarom highlighted the promising opportunities for cooperation in the academic and scientific fields, research, and development, in addition to exchanging information and skills, as well as students and organizing joint research.

He stressed the importance of promoting information exchange to respond to common cross-cutting threats and to implement standards of responsible behavior in cyberspace.

In view of the significant development of the cybersecurity sector in Israel, the number of transactions it carries out and its growing attractiveness on a global scale, a regular annual international event is organized under the name of "Cyber Week", the latest edition of which was held at Tel Aviv University last June, in cooperation with the Israeli Ministry of Foreign Affairs.

The week is an international event that provides an opportunity for experts from industry, government, defense, and academia to share their knowledge on challenges and opportunities in the field, and to discuss cyberattacks, damage to countries' critical infrastructure, public spending on information technology, the pace of spending on cyber protection, and privacy infringement.

According to the results of a study presented at the last session of the conference, spending on cybersecurity for data protection and information risk management is expected to reach $172 billion worldwide in 2022.

Another study reported that cybercrime increased significantly during the Covid 19 pandemic, and online fraud increased by more than 400% in 2020 compared to previous years, and fraudulent messages dramatically doubled as Google blocked more than 18 million malicious and phishing emails during the pandemic.

This includes scams, theft as well as the implementation of malicious tracking and spyware.

الاتحاد الاشتراكي

الأمن السيبراني: اهتمام عالمي في ارتفاع مع توالي وتيرة الهجمات الإلكترونية

تتزايد عبر العالم الحاجة إلى الأمن السيبراني لحماية الأنظمة والشبكات والبيانات، مع تسارع وتيرة التحول الرقمي للمجتمعات ومختلف الأنشطة الاقتصادية والاجتماعية، وما يكتنف ذلك أيضا من مخاطر ارتفاع وتيرة الهجمات الإلكترونية وعمليات الاحتيال والقرصنة.

وتسجل دراسات حديثة ارتفاعا مثيرا للقلق في الحرب والجرائم الإلكترونية، وتقدر أن يصل الضرر المرتبط بذلك إلى ١٠,٥ تريليون دولار سنويا بحلول عام ٢٠٢٥ على الصعيد العالمي.

وغالبا ما تهدف هذه الهجمات الإليكترونية إلى الوصول إلى المعلومات الحساسة لسرقتها أو تدميرها وتعطيل الشبكات أو الحصول على الأموال، ويفرض ذلك ارتفاع طلب الحكومات والشركات على الحلول السيبرانية، لحماية البنيات التحتية والتجهيزات والمنشآت ومختلف الأنظمة الاقتصادية والمالية وغيرها.

ويقول Ran Natanzon ران ناتازون مدير إدارة أنظمة المعلومات والابتكار بوزارة الخارجية الإسرائيلية في تصريح لوكالة المغرب العربي للأنباء، على هامش زيارة لوفد من الصحافيين الدوليين لتل أبيب، إن «الحكومات مطالبة بالمزيد من الإنفاق لحماية الشبكات والأنظمة المعلوماتية، والاستثمار في البحث العلمي السيبراني وفي الأطقم البشرية من أجل استخدام هذه الأدوات بكفاءة».

وفي إسرائيل تظهر بيانات صناعة الأمن السيبراني أنه في عام ٢٠٢١ تم تحقيق رقم معاملات وصل الى مستوى قياسي بلغ ٨,٨ مليار دولار.

ويقول الجنرال ماجور عالم الرياضيات إسحاق بن إسرائيل، المعروف بكونه أب برنامج الصناعة السيبرانية الإسرائيلي، في لقائه مع وفد الصحافيين الدوليين "باستعمال الانترنت يصبح الكل مكشوفا، فالبيانات تكون مرئية للكثيرين والأموال مكشوفة وكذلك الحياة الشخصية، والصحة والأمن علاوة على أنشطة الإدارات الحكومية".

ويضيف أن إسرائيل وضعت لنفسها أن تكون "من بين خمسة قوى كبرى في العالم في مجال الصناعة السيبرانية وترسيخ نفسها كقوة إلكترونية، ولذلك قمنا بإنشاء مركز أبحاث إلكتروني في كل جامعة، واليوم أصبحنا ندرس الأمن السيبراني في المدارس الثانوية".

هذا الاهتمام البالغ بالقطاع السيبراني يتجلي بوضوح في التطور الملفت الذي يعرفه القطب التكنولوجي الجديد بمدينة بئر السبع في صحراء النقب، والذي يضم حاليا أزيد من ٧٠ من كبريات الشركات التي توظف ما يقرب من ٢٥٠٠ شخص معظمهم مهندسو معلوميات.

يقول Ran Natanzon ران ناتازون إن الخطة الاستراتيجية للسنوات المقبلة تتوقع أن يتشكل هذا القطب من ١٥ مبنى ذكيا، يوفر عشرة آلاف وظيفة في الذكاء الاصطناعي والهندسة المعلوماتية، ومراكز جد متطورة للبحث والابتكار وللإنذار والاستجابة لهجمات الكمبيوتر، بعضها تشرف عليه فرق متخصصة من الجيش.

وضمن هذا القطب بمدينة بئر السبع تتواجد الوحدات الإلكترونية التابعة للجيش، والشركات الإسرائيلية الكبرى في المجال، خصوصا شركات البرمجيات CheckPoint و Nir Zuk's Palo Alto Networks و SentinelOne و Cybereason، علاوة على مراكز لكبريات الشركات العالمية مثل غوغل وأنتيل وميكروسوفت وغيرها.

ويضيف ران ناتازون إن مركز بئر السبع سيكون مكملا للمراكز الأخرى المتواجدة في تل أبيب وحيفا والذي يهدف لجعل إسرائيل واحدا من أكبر المراكز العالمية في المجال السيبيراني.

كما أشار إلى أن هذا التوجه سيعزز قوة قطاع البحث العلمي والتطوير والذي يمثل في إسرائيل ٤,٥ في المائة من الناتج الداخلي الخام (٢٠٢١) علما أن حصة الفرد في الناتج الداخلي الخام بلغت في الربع الرابع من ٢٠٢١ نحو ٤٤ الف و٢١٤ دولار.

ويضيف أن هذا المعدل يجعل إسرائيل تحتل الرتبة الأولى عالميا في مجال كثافة البحث العلمي والتطوير، والخامسة عالميا في كثافة التكنولوجيات الحديثة high tech density (بالنظر لعدد السكان)، فيما بلغت حصة الصادرات الإسرائيلية في مجال التكنولوجيات الدقيقة high tech نحو ٥٤ في المائة في عام ٢٠٢١، أما نسبة العاملين في قطاع التكنولوجيا العالية فقد بلغت ١٠٫٤ في المائة في مجموع القوة العاملة في عام ٢٠٢١.

ومن أجل تطوير مركز بئر السبع، تقدم المديرية الإسرائيلية للفضاء الإلكتروني دعما للشركات التي تنتقل إلى المنطقة.

ومن المدينة ذاتها يدير مركز إدارة الأحداث السيبرانية مشروع "القبة الحديدية في الدفاع السيبراني" والذي يعمل على رصد وتتبع مختلف الهجمات السيبيرانية التي تستهدف جميع مرافق البنية التحتية في إسرائيل بشكل كامل.

يقول روم ياروم Roy yarom المدير التنفيذي للسياسة والاستراتيجية بالإدارة الإسرائيلية للأمن السيبراني، في تصريح لوكالة المغرب العربي للأنباء إن مشروع «القبة الحديدية في الدفاع السيبراني" سيقدم حماية شاملة للمرافق الاقتصادية والإدارية وحتى للحواسيب الشخصية، بما يعزز الدفاع عن الفضاء الإلكتروني الإسرائيلي وتقوية بنيته في الدرع والمواجهة.

ويؤكد روم ياروم أن الإنترنت سيصبح حتما أحد أبعاد الحرب المستقبلية، إن لم يكن أهمها.

ويقول إنه يتعين أن يأخذ الجميع الأمن السيبراني على محمل الجد لأن مجرمي الإنترنت لا يستهدفون الوكالات الحكومية والمؤسسات الخاصة فقط، بل أيضا الموظفين والأشخاص العاديين وحتى الأطفال والقاصرين لأنهم أكثر قطاعات المجتمع ضعفا.

وأشار من جهة أخرى إلى أن ثمة فرصا واعدة للتعاون بين المغرب وإسرائيل في المجال السيبراني والتكنولوجيا الرقمية من أجل فضاء إلكتروني مفتوح وموثوق وآمن ومستقر.

وأبرز ياروم الفرص الواعدة للتعاون في المجال الجامعي والعلمي والبحث والتطوير، بالإضافة إلى تبادل المعلومات والمهارات، وتبادل الطلبة وتنظيم أبحاث مشتركة.

كما أكد أهمية تعزيز تبادل المعلومات من أجل الاستجابة للتهديدات الشاملة المشتركة، وتنفيذ معايير السلوك المسؤول في الفضاء السيبراني.

وبالنظر للتطور الهام الذي يعرفه قطاع الأمن السيبراني في إسرائيل، ورقم المعاملات الذي يحققه والاستقطاب المتزايد الذي يشهده عالميا أصبح يخصص له لقاء سنوي دولي منتظم تحت مسمى "الأسبوع السيبيراني" احتضنت دورته الأخيرة في ٣٠ يونيو الماضي جامعة تل أبيب بتعاون مع وزارة الخارجية الإسرائيلية.

ويعتبر هذا الأسبوع حدثا دوليا يوفر فرصة للخبراء من الصناعة والحكومات والدفاع والأوساط الأكاديمية لمشاركة معرفتهم حول التحديات والفرص في هذا المجال، ومناقشة قضايا الهجمات الإلكترونية والأضرار بالبنية التحتية الحيوية للدول، والإنفاق العام على تكنولوجيا المعلومات، ووتيرة الإنفاق على الحماية الإلكترونية، وانتهاك الخصوصية.

وبحسب نتائج إحدى الدراسات التي عرضت خلال الدورة الأخيرة من هذا المؤتمر فمن المتوقع أن يصل الإنفاق على الأمن السيبراني الموجه لحماية البيانات وإدارة المخاطر المعلوماتية إلى ١٧٣ مليار دولار على مستوى العالم في عام ٢٠٢٢.

وأفادت دراسة أخرى أن الجريمة السيبرانية ارتفعت بشكل كبير خلال جائحة كوفيد ١٩، وتزايدت عمليات الاحتيال عبر الإنترنت بأكثر من ٤٠٠ فى المائة في عام ٢٠٢٠ مقارنة بالسنوات السابقة، كما تضاعفت الرسائل الاحتيالية بشكل كبير حيث قامت غوغل بحظر أكثر من ١٨ مليون رسالة بريد إلكتروني ضارة وتصيد احتيالي يوميا خلال الجائحة، ويشمل ذلك رسائل الاحتيال والسرقة وأيضا زرع برامج خبيثة للتعقب والتجسس.

الأمن السيبراني.. اهتمام عالمي في ارتفاع مع توالي وتيرة الهجمات الإلكترونية

تتزايد عبر العالم الحاجة الى الأمن السيبراني لحماية الأنظمة والشبكات والبيانات، مع تسارع وتيرة التحول الرقمي للمجتمعات ومختلف الأنشطة الاقتصادية والاجتماعية، وما يكتنف ذلك أيضا من مخاطر ارتفاع وتيرة الهجمات الإلكترونية وعمليات الاحتيال والقرصنة.

وتسجل دراسات حديثة ارتفاعا مثيرا للقلق في الحرب والجرائم الإلكترونية، وتقدر أن يصل الضرر المرتبط بذلك إلى ١٠,٥ تريليون دولار سنويا بحلول عام ٢٠٢٥ على الصعيد العالمي.

وغالبا ما تهدف هذه الهجمات الإليكترونية إلى الوصول إلى المعلومات الحساسة لسرقتها أو تدميرها وتعطيل الشبكات أو الحصول على الأموال، ويفرض ذلك ارتفاع طلب الحكومات والشركات على الحلول السيبرانية، لحماية البنيات التحتية والتجهيزات والمنشآت ومختلف الأنظمة الاقتصادية والمالية وغيرها.

ويقول Ran Natanzon ران ناتازون مدير إدارة أنظمة المعلومات والابتكار بوزارة الخارجية الإسرائيلية في تصريح لوكالة المغرب العربي الأنباء، على هامش زيارة لوفد من الصحافيين الدوليين لتل أبيب، إن "الحكومات مطالبة بالمزيد من الإنفاق لحماية الشبكات والأنظمة المعلوماتية، والاستثمار في البحث العلمي السيبراني وفي الأطقم البشرية من أجل استخدام هذه الأدوات بكفاءة".

وفي إسرائيل تظهر بيانات صناعة الأمن السيبراني أنه في عام ٢٠٢١ تم تحقيق رقم معاملات وصل الى مستوى قياسي بلغ ٨,٨ مليار دولار.

ويقول الجنرال ماجور عالم الرياضيات إسحاق بن إسرائيل، المعروف بكونه أب برنامج الصناعة السيبرانية الإسرائيلي، في لقائه مع وفد الصحافيين الدوليين "باستعمال الانترنت يصبح الكل مكشوفا، فالبيانات تكون مرئية للكثيرين والأموال مكشوفة وكذلك الحياة الشخصية، والصحة والأمن علاوة على أنشطة الإدارات الحكومية".

ويضيف أن إسرائيل وضعت لنفسها أن تكون "من بين خمسة قوى كبرى في العالم في مجال الصناعة السيبرانية وترسيخ نفسها كقوة إلكترونية، ولذلك قمنا بإنشاء مركز أبحاث إلكتروني في كل جامعة، واليوم أصبحنا ندرس الأمن السيبراني في المدارس الثانوية".

هذا الاهتمام البالغ بالقطاع السيبراني يتجلي بوضوح في التطور الملفت الذي يعرفه القطب التكنولوجي الجديد بمدينة بئر السبع في صحراء النقب، والذي يضم حاليا أزيد من ٧٠ من كبريات الشركات التي توظف ما يقرب من ٢٥٠٠ شخص معظمهم مهندسو معلوميات.

يقول Ran Natanzon ران ناتازون إن الخطة الاستراتيجية للسنوات المقبلة تتوقع أن يتشكل هذا القطب من ١٥ مبنى ذكيا، يوفر عشرة آلاف وظيفة في الذكاء الاصطناعي والهندسة المعلوماتية، ومراكز جد متطورة للبحث والابتكار وللإنذار والاستجابة لهجمات الكمبيوتر، بعضها تشرف عليه فرق متخصصة من الجيش.

وضمن هذا القطب بمدينة بئر السبع تتواجد الوحدات الإلكترونية التابعة للجيش، والشركات الإسرائيلية الكبرى في المجال، خصوصا شركات البرمجيات CheckPoint و Nir Zuk's Palo Alto Networks و SentinelOne و Cybereason، علاوة على مراكز لكبريات الشركات العالمية مثل غوغل وأنتيل وميكروسوفت وغيرها.

ويضيف ران ناتازون إن مركز بئر السبع سيكون مكملا للمراكز الأخرى المتواجدة في تل أبيب وحيفا والذي يهدف لجعل إسرائيل واحدا من أكبر المراكز العالمية في المجال السيبيراني.

كما أشار الى أن هذا التوجه سيعزز قوة قطاع البحث العلمي والتطوير والذي يمثل في إسرائيل ٥ر٤ في المائة من الناتج الداخلي الخام (٢٠٢١) علما أن حصة الفرد في الناتج الداخلي الخام بلغت في الربع الرابع من ٢٠٢١ نحو ٤٤ الف و٢١٤ دولار.

ويضيف أن هذا المعدل يجعل إسرائيل تحتل الرتبة الأولى عالميا في مجال كثافة البحث العلمي والتطوير، والخامسة عالميا في كثافة التكنولوجيات الحديثة high tech density (بالنظر لعدد السكان)، فيما بلغت حصة الصادرات الإسرائيلية في مجال التكنولوجيات الدقيقة high tech نحو ٥٤ في المائة في عام ٢٠٢١، أما نسبة العاملين في قطاع التكنولوجيا العالية فقد بلغت ٤ر١٠ في المائة في مجموع القوة العاملة في عام ٢٠٢١.

ومن أجل تطوير مركز بئر السبع، تقدم المديرية الإسرائيلية للفضاء الإلكتروني دعما للشركات التي تنتقل إلى المنطقة.

ومن المدينة ذاتها يدير مركز إدارة الأحداث السيبرانية مشروع "القبة الحديدية في الدفاع السيبراني" والذي يعمل على رصد وتتبع مختلف الهجمات السيبيرانية التي تستهدف جميع مرافق البنية التحتية في إسرائيل بشكل كامل.

يقول روم ياروم Roy yarom المدير التنفيذي للسياسة والاستراتيجية بالإدارة الإسرائيلية للأمن السيبراني، في تصريح لوكالة المغرب العربي للأنباء إن مشروع "القبة الحديدية في الدفاع السيبراني" سيقدم حماية شاملة للمرافق الاقتصادية والإدارية وحتى للحواسيب الشخصية، بما يعزز الدفاع عن الفضاء الإلكتروني الإسرائيلي وتقوية بنيته في الدرع والمواجهة.

ويؤكد روم ياروم أن الإنترنت سيصبح حتما أحد أبعاد الحرب المستقبلية،

لم يكن أهمها.

ويقول إنه يتعين أن يأخذ الجميع الأمن السيبراني على محمل الجد لأن مجرمي الإنترنت لا يستهدفون الوكالات الحكومية والمؤسسات الخاصة فقط، بل أيضا الموظفين والأشخاص العاديين وحتى الأطفال والقاصرين لأنهم أكثر قطاعات المجتمع ضعفا.

وأشار من جهة أخرى الى أن ثمة فرصا واعدة للتعاون بين المغرب وإسرائيل في المجال السيبراني والتكنولوجيا الرقمية من أجل فضاء إلكتروني مفتوح وموثوق وآمن ومستقر.

وأبرز ياروم الفرص الواعدة للتعاون في المجال الجامعي والعلمي والبحث والتطوير، بالإضافة إلى تبادل المعلومات والمهارات، وتبادل الطلبة وتنظيم أبحاث مشتركة.

كما أكد أهمية تعزيز تبادل المعلومات من أجل الاستجابة للتهديدات الشاملة المشتركة، وتنفيذ معايير السلوك المسؤول في الفضاء السيبراني.

وبالنظر للتطور الهام الذي يعرفه قطاع الأمن السيبراني في إسرائيل، ورقم المعاملات الذي يحققه والاستقطاب المتزايد الذي يشهده عالميا أصبح يخصص له لقاء سنوي دولي منتظم تحت مسمى "الأسبوع السيبيراني" احتضنت دورته الأخيرة في ٣٠ يونيو الماضي جامعة تل أبيب بتعاون مع وزارة الخارجية الإسرائيلية.

ويعتبر هذا الأسبوع حدثا دوليا يوفر فرصة للخبراء من الصناعة والحكومات والدفاع والأوساط الأكاديمية لمشاركة معرفتهم حول التحديات والفرص في هذا المجال، ومناقشة قضايا الهجمات الإلكترونية والأضرار بالبنية التحتية الحيوية للدول، والإنفاق العام على تكنولوجيا المعلومات، ووتيرة الإنفاق على الحماية الإلكترونية، وانتهاك الخصوصية.

وبحسب نتائج إحدى الدراسات التي عرضت خلال الدورة الأخيرة من هذا المؤتمر فمن المتوقع أن يصل الإنفاق على الأمن السيبراني الموجه لحماية البيانات وإدارة المخاطر المعلوماتية إلى ١٧٣ مليار دولار على مستوى العالم في عام ٢٠٢٢.

وأفادت دراسة أخرى أن الجريمة السيبرانية ارتفعت بشكل كبير خلال جائحة كوفيد ١٩، وتزايدت عمليات الاحتيال عبر الإنترنت بأكثر من ٤٠٠ فى المائة في عام ٢٠٢٠ مقارنة بالسنوات السابقة، كما تضاعفت الرسائل الاحتيالية بشكل كبير حيث قامت غوغل بحظر أكثر من ١٨ مليون رسالة بريد إلكتروني ضارة وتصيد احتيالي يوميا خلال الجائحة، ويشمل ذلك رسائل الاحتيال والسرقة وأيضا زرع برامج خبيثة للتعقب والتجسس .

الأمن السيبراني : اهتمام عالمي في ارتفاع مع توالي وتيرة الهجمات الإلكترونية

ومع/بقلم عبد الرزاق طريبق

تتزايد عبر العالم الحاجة الى الأمن السيبراني لحماية الأنظمة والشبكات والبيانات، مع تسارع وتيرة التحول الرقمي للمجتمعات ومختلف الأنشطة الاقتصادية والاجتماعية، وما يكتنف ذلك أيضا من مخاطر ارتفاع وتيرة الهجمات الإلكترونية وعمليات الاحتيال والقرصنة.

وتسجل دراسات حديثة ارتفاعا مثيرا للقلق في الحرب والجرائم الإلكترونية، وتقدر أن يصل الضرر المرتبط بذلك إلى ١٠,٥ تريليون دولار سنويا بحلول عام ٢٠٢٥ على الصعيد العالمي.

وغالبا ما تهدف هذه الهجمات الإليكترونية إلى الوصول إلى المعلومات الحساسة لسرقتها أو تدميرها وتعطيل الشبكات أو الحصول على الأموال، ويفرض ذلك ارتفاع طلب الحكومات والشركات على الحلول السيبرانية، لحماية البنيات التحتية والتجهيزات والمنشآت ومختلف الأنظمة الاقتصادية والمالية وغيرها.

ويقول Ran Natanzon ران ناتازون مدير إدارة أنظمة المعلومات والابتكار بوزارة الخارجية الإسرائيلية في تصريح لوكالة المغرب العربي الأنباء، على هامش زيارة لوفد من الصحافيين الدوليين لتل أبيب، إن "الحكومات مطالبة بالمزيد من الإنفاق لحماية الشبكات والأنظمة المعلوماتية، والاستثمار في البحث العلمي السيبراني وفي الأطقم البشرية من أجل استخدام هذه الأدوات بكفاءة".

وفي إسرائيل تظهر بيانات صناعة الأمن السيبراني أنه في عام ٢٠٢١ تم تحقيق رقم معاملات وصل الى مستوى قياسي بلغ ٨,٨ مليار دولار.

ويقول الجنرال ماجور عالم الرياضيات إسحاق بن إسرائيل، المعروف بكونه أب برنامج الصناعة السيبرانية الإسرائيلي، في لقائه مع وفد الصحافيين الدوليين "باستعمال الانترنت يصبح الكل مكشوفا، فالبيانات تكون مرئية للكثيرين والأموال مكشوفة وكذلك الحياة الشخصية، والصحة والأمن علاوة على أنشطة الإدارات الحكومية".

ويضيف أن إسرائيل وضعت لنفسها أن تكون "من بين خمسة قوى كبرى في العالم في مجال الصناعة السيبرانية وترسيخ نفسها كقوة إلكترونية، ولذلك قمنا بإنشاء مركز أبحاث إلكتروني في كل جامعة، واليوم أصبحنا ندرس الأمن السيبراني في المدارس الثانوية".

هذا الاهتمام البالغ بالقطاع السيبراني يتجلي بوضوح في التطور الملفت الذي يعرفه القطب التكنولوجي الجديد بمدينة بئر السبع في صحراء النقب، والذي يضم حاليا أزيد من ٧٠ من كبريات الشركات التي توظف ما يقرب من ٢٥٠٠ شخص معظمهم مهندسو معلوميات.

يقول Ran Natanzon ران ناتازون إن الخطة الاستراتيجية للسنوات المقبلة تتوقع أن يتشكل هذا القطب من ١٥ مبنى ذكيا، يوفر عشرة آلاف وظيفة في الذكاء الاصطناعي والهندسة المعلوماتية، ومراكز جد متطورة للبحث والابتكار وللإنذار والاستجابة لهجمات الكمبيوتر، بعضها تشرف عليه فرق متخصصة من الجيش.

وضمن هذا القطب بمدينة بئر السبع تتواجد الوحدات الإلكترونية التابعة للجيش، والشركات الاسرائيلية الكبرى في المجال، خصوصا شركات البرمجيات CheckPoint و Nir Zuk's Palo Alto Networks و SentinelOne و Cybereason، علاوة على مراكز لكبريات الشركات العالمية مثل غوغل وأنتيل وميكروسوفت وغيرها.

ويضيف ران ناتازون إن مركز بئر السبع سيكون مكملا للمراكز الأخرى المتواجدة في تل أبيب وحيفا والذي يهدف لجعل إسرائيل واحدا من أكبر المراكز العالمية في المجال السيبيراني.

كما أشار الى أن هذا التوجه سيعزز قوة قطاع البحث العلمي والتطوير والذي يمثل في إسرائيل ٥ر٤ في المائة من الناتج الداخلي الخام (٢٠٢١) علما أن حصة الفرد في الناتج الداخلي الخام بلغت في الربع الرابع من ٢٠٢١ نحو ٤٤ الف و٢١٤ دولار.

ويضيف أن هذا المعدل يجعل إسرائيل تحتل الرتبة الأولى عالميا في مجال كثافة البحث العلمي والتطوير، والخامسة عالميا في كثافة التكنولوجيات الحديثة high tech density (بالنظر لعدد السكان)، فيما بلغت حصة الصادرات الإسرائيلية في مجال التكنولوجيات الدقيقة high tech نحو ٥٤ في المائة في عام ٢٠٢١، أما نسبة العاملين في قطاع التكنولوجيا العالية فقد بلغت ٤ر١٠ في المائة في مجموع القوة العاملة في عام ٢٠٢١.

ومن أجل تطوير مركز بئر السبع، تقدم المديرية الإسرائيلية للفضاء الإلكتروني دعما للشركات التي تنتقل إلى المنطقة.

ومن المدينة ذاتها يدير مركز إدارة الأحداث السيبرانية مشروع "القبة الحديدية في الدفاع السيبراني" والذي يعمل على رصد وتتبع مختلف الهجمات السيبيرانية التي تستهدف جميع مرافق البنية التحتية في إسرائيل بشكل كامل.

يقول روم ياروم Roy yarom المدير التنفيذي للسياسة والاستراتيجية بالإدارة الإسرائيلية للأمن السيبراني، في تصريح لوكالة المغرب العربي للأنباء إن مشروع "القبة الحديدية في الدفاع السيبراني" سيقدم حماية شاملة للمرافق الاقتصادية والإدارية وحتى للحواسيب الشخصية، بما يعزز الدفاع عن الفضاء الإلكتروني الإسرائيلي وتقوية بنيته في الدرع والمواجهة.

ويؤكد روم ياروم أن الإنترنت سيصبح حتما أحد أبعاد الحرب المستقبلية، إن لم يكن أهمها.

ويقول إنه يتعين أن يأخذ الجميع الأمن السيبراني على محمل الجد لأن مجرمي الإنترنت لا يستهدفون الوكالات الحكومية والمؤسسات الخاصة فقط، بل أيضا الموظفين والأشخاص العاديين وحتى الأطفال والقاصرين لأنهم أكثر قطاعات المجتمع ضعفا.

وأشار من جهة أخرى الى أن ثمة فرصا واعدة للتعاون بين المغرب وإسرائيل في المجال السيبراني والتكنولوجيا الرقمية من أجل فضاء إلكتروني مفتوح وموثوق وآمن ومستقر.

وأبرز ياروم الفرص الواعدة للتعاون في المجال الجامعي والعلمي والبحث والتطوير، بالإضافة إلى تبادل المعلومات والمهارات، وتبادل الطلبة وتنظيم أبحاث مشتركة.

كما أكد أهمية تعزيز تبادل المعلومات من أجل الاستجابة للتهديدات الشاملة المشتركة، وتنفيذ معايير السلوك المسؤول في الفضاء السيبراني.

وبالنظر للتطور الهام الذي يعرفه قطاع الأمن السيبراني في إسرائيل، ورقم المعاملات الذي يحققه والاستقطاب المتزايد الذي يشهده عالميا أصبح يخصص له لقاء سنوي دولي منتظم تحت مسمى "الأسبوع السيبيراني" احتضنت دورته الأخيرة في ٣٠ يونيو الماضي جامعة تل أبيب بتعاون مع وزارة الخارجية الإسرائيلية.

ويعتبر هذا الأسبوع حدثا دوليا يوفر فرصة للخبراء من الصناعة والحكومات والدفاع والأوساط الأكاديمية لمشاركة معرفتهم حول التحديات والفرص في هذا المجال، ومناقشة قضايا الهجمات الإلكترونية والأضرار بالبنية التحتية الحيوية للدول، والإنفاق العام على تكنولوجيا المعلومات، ووتيرة الإنفاق على الحماية الإلكترونية، وانتهاك الخصوصية.

وبحسب نتائج إحدى الدراسات التي عرضت خلال الدورة الأخيرة من هذا المؤتمر فمن المتوقع أن يصل الإنفاق على الأمن السيبراني الموجه لحماية البيانات وإدارة المخاطر المعلوماتية إلى ١٧٢ مليار دولار على مستوى العالم في عام ٢٠٢٢.

وأفادت دراسة أخرى أن الجريمة السيبرانية ارتفعت بشكل كبير خلال جائحة كوفيد ١٩، وتزايدت عمليات الاحتيال عبر الإنترنت بأكثر من ٤٠٠ فى المائة في عام ٢٠٢٠ مقارنة بالسنوات السابقة، كما تضاعفت الرسائل الاحتيالية بشكل كبير حيث قامت غوغل بحظر أكثر من ١٨ مليون رسالة بريد إلكتروني ضارة وتصيد احتيالي يوميا خلال الجائحة، ويشمل ذلك رسائل الاحتيال والسرقة وأيضا زرع برامج خبيثة للتعقب والتجسس.

ไทยรัฐ ออนไลน์

Israel once is not enough (1)

As the world faces a huge challenge from COVID-19, Israel is one of the countries that has managed to cope with and cope with the devastating pandemic of the virus that has been closely monitored around the world. In particular, it was a rapid pioneer in public vaccination programs, being among the first countries to initiate vaccination certificates or the Green Pass to keep society and business moving forward. Including being the first nation to launch injection booster vaccine Even confident that they are ready to accept tourists from all over the world, whether they are vaccinated against COVID-19. come or not without having to test for infection by PCR before arrival And do not have to detain from 21 May after opening the border in March. Tourists, after receiving a visa, just fill out the Israel Entry Form. Check details at https://israelsafe.com/ and that's the end of the story.

Israel is a small country in the Middle East connecting Europe, Asia and Africa, located on the eastern coast of the Mediterranean Sea. Bordering Egypt, Jordan, Lebanon and Syria, it is a land with a long and complicated history. With the diversity of races, religions and cultures merging into a distinctive charm. At the same time, there are unique landscapes, including valleys, mountains, deserts, lakes, grasslands, forests and coastlines. making it one of the must-visit destinations. In the past, we have only heard news of war and conflict. obscure the fact that Israel is one of the great powers of innovation and technology. as well as being a production center for world-class entrepreneurs until being called "Start-up Nation"

The first place that must be visited is inevitable , " Tel Aviv " , the coolest city of the Mediterranean. One of the bustling cities full of life. Plus the trailer with the 6th highest cost of living in the world. With 14 kilometers of soft white beaches stretching along the Mediterranean coast with almost year-round sunshine. making it possible to see the atmosphere of people doing outdoor activities uninterrupted This old city that has been nicknamed The "city that doesn't sleep" boasts pub bars at night. Coffee shop - stylish food wheeling with retro architecture Let's talk about the other side of Tel Aviv next time. Take us back to the ancient atmosphere at the " Old Jaffa " district, home to one of the oldest harbors in the world from thousands of years to the present.

ไทยรัฐ ออนไลน์

Israel once is not enough (2)

Last time I had the opportunity to tell you about my experience of visiting Tel Aviv, Israel 's second largest city, although it was only a short time, but I felt the color, the energetic, lively, full of energy. The meaning of the city is " Hill of Spring ", while passing through the residential areas, you can feel the peace and security. You can see people walking their dogs along the community in a familiar way. until a local Israelite told him, This cool city is not only a source of technology experts. It is recognized as having one of the best startup ecosystems in the world. It also ranks among the top dog and pet friendly cities.

From Tel Aviv's cutting edge We're heading south. To return to the atmosphere of the ancient world at the district " Jaffa " , also known as " Yafo " , which is one of the oldest port cities in the world. From more than 4,000 years ago it was an important transport route in the past to the late 19th century by Jews from around the world returning to their ancestral homeland of Israel via the port of Jaffa until the end of the 19th century. A port for local fishing boats and small yachts to date.

This area is located on a hill. overlooking the Mediterranean Sea up close It is unique from a long history. Importantly, it is a harmonious community of Muslims, Christians, and Jews. In addition, the Bible states that Japheth, the son of Noah, found a beautiful hill overlooking the water. therefore chose to settle Until later became a famous city in the reign of King Solomon. of Israel in 950 B.C.

was restored to its glorious past in 1968 as a cultural and entertainment hub. It doesn't take long to walk through small winding alleyways. surrounded by houses made of stone But you can feel the atmosphere of the ancient city that is magical. This may be because Jaffa doesn't have a rich religious history like the old city of Jerusalem. So it's easy to explore and fall in love with Jaffa.

ไทยรัฐ ออนไลน์

Open the world of "Cyber Threats" in Israel

It is undeniable that computers The Internet, digital media, and social networks play an important role in life in all walks of life. whether it is a personal matter in general like communication spending make financial transactions Mass storage of personal data of an organization to control the use of electronic devices via the Internet and the pandemic of COVID-19 That is a great challenge for humanity, severely affecting people around the world. both living and working Stimulate the use of digital technology by leaps and bounds.

And when using the Internet, it opens the door to cyber attacks at any time and in any form. Cybercriminals are not only targeting individuals. but also focus on public infrastructure systems as well as private businesses with money as an incentive "Cyber security" is therefore not a distant matter, but is an issue that all parties must focus on.

At the international conference on "Cyber Security" or " Cyber Week " , a large annual event that has been regarded as the most recognized important "event" in the world. Under the cooperation of the Cyberblavatnik Center (ICRC), the Yuval Neman Science, Technology and Security Workshop, Tel Aviv University, Israel National Cyber Directorate within Under the Prime Minister's Office and the Israeli Foreign Ministry co-hosted the event from 27-30 June at Tel Aviv University. in Tel Aviv Israel's second largest city, known by many as the "Silicon Valley of the Middle East," is one of the hottest and most advanced technology hubs in the world.

The event provides opportunities for experts from the industry. government agency academic soldier educational institution Including startups, investors, as well as more than 9,000 diplomats of all genders and ages from 80 countries to present innovations, exchange knowledge and technology. Share experiences and challenges from the dilemma. "Cyber threats" are becoming more and more complex and serious. as well as open a forum on a variety of issues to stimulate new ideas. in the most energetic and energetic atmosphere And most importantly, the international news team of Thairath Newspaper also received a special opportunity from the "Embassy of Israel in Thailand" to be one of the media from a few countries to learn from this event as well.

In 2021, ransomware attacks occur every 11 seconds, compared to every 39 seconds in 2019, with almost half of cyber attacks in 2021 targeting small and medium-sized businesses. The damage amount is up to 20 billion dollars. And attacks will also increase by 400 percent during the coronavirus pandemic in 2021, with the average cost to recover $1.85 million, or about 66.6 million baht, more than double from 2019. Cyber-related damage will reach $10.5 trillion annually by 2025, while cybersecurity spending could reach $172 billion globally by 2022.

One of the key figures speaking at the event was Israeli Defense Minister Benny Gantz. that sums up the dynamics of the growing and increasingly violent cyber conflict. It also stressed the need for private companies to follow government guidelines and cooperate to prevent potential risks. It also clearly stated that "Iran" is a key player in cyberattacks. This was originally a global challenge and later a regional challenge. Even in the end poses a threat to Israel.

The highlight of the opening day of the first day was the queue of Prime Minister Naftali Bennett that day. who currently stepped down from office after serving only a year and announced the dissolution of the parliament Prepare to hold the fifth general election in three and a half years and pass the wood to Mr. Yail Lapid, Minister of Foreign Affairs Acting as the Prime Minister By Bennett emphasizes the The importance of global cooperation for cybersecurity especially sharing knowledge and experiences with friends. and warned that Israel has never had a policy of harming or offending anyone. But if anyone attempting a cyber attack against Israel must "Receive the consequences of that action."

Bennett also said that "Cyber has become the future dimension of warfare. Instead of sending troops to risk their lives in battle outside. It just takes a group of people to fight behind a computer anywhere in the world without risking their lives."

Before the end of the keynote, Bennett also gave advice to the full auditorium attendees, most of them CEOs. Corporate executives, experts and representatives from various departments from around the world that When deciding what to do, you need to act quickly, without hesitation, and try to find a way to get the right information. And finally, don't play politics.

ไทยรัฐ ออนไลน์

"Cyber Dome" Fights Threats

Cybersecurity threats have been a hot topic that has been heard a lot in recent years. Whether it is an attack from viruses, hackers , as well as malware. Especially in today's era where the world is driven by internet technology and the COVID-19 outbreak. That pushes people around the world to change their lifestyles to live in the digital world by leaps and bounds. Cyber attacks are thus undeniably growing in shadow. Meanwhile, Russia's invasion of Ukraine exemplifies the urgent global awareness of the importance of cybersecurity.

Israel, one of the leading countries in technology innovation, has one of the highest venture capital investments in the world by population (or about 5.4 percent), becoming the center of the cybersecurity ecosystem over the course of the year. 2021 has raised a record $8.8 billion in startup funding. One-third of cybersecurity unicorn startups worldwide, or 33 percent, are based in Israel. Still, it is affected more frequently by cyberattacks than countries like France, Japan, the US and Germany, according to Israeli cybersecurity firm Check Point.

The results showed that Cyber attacks targeting Israel increased 92 percent from the previous year. Globally, it increased by around 50 percent, especially in the second half of the year, with an average global cyberattack of 925 per week. The industries most affected are Education/research, followed by government/military agencies. communication company and internet service providers, followed by public health services All of these hits increased by at least 47 percent, while the trend of email-targeted attacks also saw a marked increase.

Check Point also revealed that the major threats currently come in the form of Business Email Compromise (BEC), or email attacks to trick individuals in an organization into transferring money or for identity theft. This is often aimed at individuals or small entities and attacks on the supply chain. in the case of hacking "Solar Winds" to infiltrate the information of many government agencies, private companies, think tanks. a few years ago including ransomware or ransom hacks that see a shift in targeting from individual attacks to more organizations.

And when the digital attack intensifies Israel's cyber army has therefore restructured its combat operations from "Cyber Resi lience," or "Preparation," to respond and restore its systems to "Proactive Defense." Hunt for cyber attackers No matter where you are hiding in the digital world without interference. At the same time, the importance of preparation "Cybersecurity protocols" for infrastructure for broad public use. This includes providing effective resources and transferring necessary skills to the entire private sector. Build capacity to participate in all dimensions of cyber defense.

Gaby Portnoy, director of the Israel National Cyber Directorate (INCD), unveiled plans for a major public speech for the first time since his appointment in August. At the end of last month, Cyber Week 2022, an annual event held at Tel Aviv University in Tel Aviv, Israel. By presenting the project "Cyber Dome" (Cyber Dome), INCD's initiative to enhance the fight against cyber threatAll forms while acting as Big Data and Artificial Intelligence to work together. Detect real-time national cyber attacks do an analysis and mitigate the dangers of cyber-attacks. Proactively protect national assets as a whole, just like the "Iron Dome" (Iron Dome) short-range air defense system with cutting-edge technology to identify and destroy threats before they cause damage.

Although more than 1,500 cyberattacks were detected and stopped in the past year, INCD still believes it is imperative to intensify its defenses, so the "cyber dome" is the answer. Various attack challenges

format and extend to private hacker groups hired gunner independent organized crime And even individuals, while the main "antagonist" in Israel's cyberspace is Iran, alongside Hezbollah and Hamas. The most effective cybersecurity is not a "technology" in the world, but a "collaboration".

"You cannot fight cyber invasion alone. You need partners at home, in your community, in governments, across sectors, including educational institutions, the private sector, and allies around the world."

Cyber Week

June 27th-30th, 2022

Tel Aviv University, Israel

Yuval Ne'eman Workshop for Science, Technology and Security Tel Aviv University

Blavatnik Interdisciplinary Cyber Research Center

TEL AVIV UNIVERSITY אוניברסיטת תל אביב

Cyber Israel National Cyber Directorate

In cooperation with: Ministry of Foreign Affairs Israel · ISRAEL CYBER ALLIANCE · State of Israel Ministry of Economy and Industry Foreign Trade Administration · ISRAEL EXPORT INSTITUTE

ไทยรัฐ ออนไลน์

وكالة المغرب العربي للأنباء MAP AGENCE MAROCAINE DE PRESSE

Join the Cyber Defense

Israel was one of the first nations to commit to building a body of knowledge in cybertechnology, making it not limited to intelligence and security purposes. but also open to research studies Business development including application in daily life Until there is a breakthrough in innovation at the top level in the world. And with the idea that dealing with and fighting criminals online cannot be accomplished alone. requires cooperation Share knowledge and experience It is therefore the origin of the cooperation in cyber defense of Israel and friends around the world.

at the beginning of last month The Israeli National Cyber Office and the National Cybersecurity Commission (NSC) have signed a "MoU on Cooperation on Cybersecurity" by Israeli Ambassador Orna Zaif. in Thailand On behalf of the Israeli National Cyber Office and General Prachya Chalermwat, Secretary-General of the NBTC, this marks the beginning of cooperation for the development of cybersecurity between Israel and Thailand.

Mrs. Sakif said Through years of intense fighting experience, Israel knows who its enemies are and where their borders are. But cyber attacks In addition to the location is not specified, it is also without borders. This requires cooperation and sharing of experiences. In order to effectively tackle this threat, the signing also marked the friendship and trust between the two nations, which the embassy served as a bridge to help both sides face common challenges. more strongly

The upcoming cooperation activities include the exchange of knowledge and events. to personnel development, both on study tours and cyber seminars and facilitating various activities to further strengthen the potential in the future.

Amornda Ponguthai

Cyber Security: Global Attention on the Rise as Cyber Attacks Escalate

The need for cybersecurity to protect systems, networks and data is increasing worldwide, with the accelerating digital transformation of societies and various economic and social activities, as well as the risks of mass cyber attacks, fraud and hacking.

Recent studies reveal an alarming rise in war and cybercrime, and estimate that the associated damage will reach $10.5 trillion annually by 2025 globally.

Cyber attacks are often aimed at accessing sensitive information to steal or destroy it, disrupt networks or obtain funds.

Faced with this situation, governments and companies are opting for cybersecurity solutions to protect infrastructure, equipment, facilities, and various economic and financial systems.

"Governments are required to work more to protect networks and information systems, and to invest in cyber scientific research and human capital in order to efficiently use these tools," Ran Natanzon, Head of innovation & Country branding, Public Diplomacy Division at Ministry of Foreign Affairs of Israel, told MAP on the sidelines of a visit of a delegation of international journalists to Tel Aviv.

In Israel, cyber industry data show that in 2021, a significant number of transactions were made, reaching a record level of $8.8 billion.

For his part, Major General and mathematician Issac Ben-Israel, a pioneer in Israel's cyber-industry program, said that "with the use of the Internet, 'everything becomes exposed'. Data is visible, and funds are discovered, as well as privacy, health and security, in addition to the activities of government administrations".

He added that Israel sets itself to be "among the five major powers in the world in the field of cyberindustry and stands out as an electronic force, and that is why we have established an electronic research center in every university, and today we teach cybersecurity in secondary schools."

This interest in the cyber sector is most evident in the remarkable development of the new technological pole in the city of Beersheba in the Negev desert, which currently hosts more than 70 of the largest companies employing nearly 2,500 people, most of whom are information engineers.

Ran Natanzon indicated that the strategic plan for the coming years foresees that this center will include 15 intelligent buildings, providing about ten thousand jobs in artificial intelligence and computer engineering, and highly developed centers for research, innovation, alert and response to computer attacks, some of which will be under the supervision of specialized teams from the army.

This pole in the city of Beersheba also houses the electronic units of the army and the major Israeli companies in the field, especially the software companies CheckPoint, Nir Zuk's Palo Alto Networks, SentinelOne and Cybereason,

in addition to centers of the largest international companies such as Google, Intel, and Microsoft, among others.

Ran Natason pointed out that the Beersheba center complements the others in Tel Aviv and Haifa, which aim to make Israel one of the world's leading countries in the field of cybersecurity.

He also stressed that this trend will strengthen the scientific research and development sector, which in Israel represents 5.4% of the gross domestic product (GDP) (2021), given the fact that the per capita GDP amounted to 44,214 dollars in the fourth quarter of 2021.

This rate places Israel at the top world rank in terms of scientific research and development intensity, and at the fifth world rank in modern technology density (per population), while the share of Israeli exports in the high-tech sector has reached about 54 percent in 2021.

As for the percentage of workers in the high-tech sector, it reached 10.4 percent of the total workforce in 2021.

To develop the Beersheba Center, Israel's Cyberspace Directorate provides support to companies that set up shop in the area.

From the same city, the National Cyber Directorate manages the "Iron Dome in Cyber Defense" project, which aims to monitor and track various cyber attacks that target all infrastructure in Israel.

In a statement to MAP, Roy Yarom, executive director of policy and strategy at the Israeli Department of Cybersecurity, said that the "Iron Dome in Cyber Defense" project will provide comprehensive protection of economic and administrative facilities, and even personal computers, in a way that enhances the defense of Israeli cyberspace and strengthens its structure in both shielding and confrontation.

Rom Yarom pointed out that the Internet will inevitably become one of the dimensions of future warfare, if not the most important.

He said that everyone should take cybersecurity seriously because cybercriminals target not only government agencies and private institutions, but also employees, ordinary people, and even children and minors because they are the most vulnerable sectors of society.

On the other hand, he stressed that there are promising opportunities for cooperation between Morocco and Israel in the cyber and digital field for open, reliable, secure, and stable cyberspace.

Yarom highlighted the promising opportunities for cooperation in the academic and scientific fields, research, and development, in addition to exchanging information and skills, as well as students and organizing joint research.

He stressed the importance of promoting information exchange to respond to common cross-cutting threats and to implement standards of responsible behavior in cyberspace.

In view of the significant development of the cybersecurity sector in Israel, the number of transactions it carries out and its growing attractiveness on a global scale, a regular annual international event is organized under the name of "Cyber Week", the latest edition of which was held at Tel Aviv University last June, in cooperation with the Israeli Ministry of Foreign Affairs.

The week is an international event that provides an opportunity for experts from industry, government, defense, and academia to share their knowledge on challenges and opportunities in the field, and to discuss cyberattacks, damage to countries' critical infrastructure, public spending on information technology, the pace of spending on cyber protection, and privacy infringement.

According to the results of a study presented at the last session of the conference, spending on cybersecurity for data protection and information risk management is expected to reach $172 billion worldwide in 2022.

Another study reported that cybercrime increased significantly during the Covid 19 pandemic, and online fraud increased by more than 400% in 2020 compared to previous years, and fraudulent messages dramatically doubled as Google blocked more than 18 million malicious and phishing emails during the pandemic.

This includes scams, theft as well as the implementation of malicious tracking and spyware.

وكالة المغرب العربي للأنباء
MAP
AGENCE MAROCAINE DE PRESSE

Cybersécurité: Un intérêt mondial croissant face aux nombreuses cyberattaques

Tel-Aviv – A travers le monde, la cybersécurité s'avère de plus en plus importante dans la protection des systèmes, des réseaux et des données, d'autant plus que l'accélération de la transformation numérique des sociétés et des diverses activités économiques et sociales, s'accompagne, le plus souvent, de risques élevés des cyberattaques, de fraude et de piratage.

Des études récentes démontrent une augmentation "alarmante" de cyber-guerre et de la cybercriminalité, estimant que les dommages y afférents atteindront annuellement les 10,5 trillions de dollars en 2025.

Les cyber-attaques visent souvent à accéder à des informations sensibles pour les voler ou les détruire, perturber les réseaux ou obtenir des fonds.

Face à ces données, les gouvernements et les entreprises optent pour des solutions de cybersécurité, dans le dessein de protéger les infrastructures, les équipements, les installations, ainsi que les différents systèmes économiques et financiers.

Dans ce sens, Ran Natanzon, directeur du Département des systèmes d'information et de l'innovation au ministère israélien des Affaires étrangères, a confié à la MAP, en marge de la visite d'une délégation de journalistes internationaux à Tel-Aviv, que "les gouvernements sont appelés à dépenser davantage pour protéger les réseaux et les systèmes d'information, et à investir dans la recherche scientifique cybernétique et le capital humain pour une exploitation efficace de ces outils".

En Israël, les données de la cyber-industrie relèvent qu'en 2021, un nombre important de transactions a été réalisé, atteignant un niveau record de 8,8 milliards de dollars.

De son côté, le major-général et mathématicien, Issac Ben-Israel, un pionnier du programme de la cyber-industrie en Israël, a indiqué qu'"avec l'utilisation d'Internet, +tout devient exposé+. Les données sont visibles, et les fonds sont découverts, au même titre que la vie privée, la santé et la sécurité, en plus des activités des administrations gouvernementales".

"Israël s'est fixé l'objectif de faire partie des cinq grandes puissances mondiales dans le domaine de la cyber-industrie et s'imposer comme une force en la matière. C'est pourquoi, nous avons établi un centre de recherche électronique dans chaque université, et aujourd'hui nous enseignons la cybersécurité dans les écoles secondaires", a-t-il mis en avant.

Ce grand intérêt pour le secteur cybernétique se manifeste clairement dans le développement remarquable du nouveau pôle technologique de la ville de Beer-Sheva dans le désert du Néguev, qui comprend actuellement plus de 70 grandes entreprises employant environ 2.500 personnes, dont la plupart des ingénieurs en informatique.

Ainsi, Ran Natanzon indique que le plan stratégique pour les années à venir prévoit que ce pôle comprendra 15 bâtiments intelligents, fournissant une dizaine de milliers d'emplois en intelligence artificielle et en ingénierie informatique, et des centres très développés de recherche, d'innovation, d'alerte et de riposte aux attaques informatiques, dont certains seront sous la supervision d'équipes spécialisées de l'armée.

Le pôle de la ville de Beer-Sheva abrite les unités électroniques de l'armée et les grandes entreprises israéliennes, notamment les éditeurs de logiciels CheckPoint, Palo Alto Networks de Nir Zuk, SentinelOne et Cybereason, ainsi que les centres des grandes entreprises internationales telles que Google, Intel, Microsoft, entre autres.

Le Centre de Beer-Sheva vient, ainsi, compléter les autres de Tel-Aviv et de Haïfa, qui visent à faire d'Israël l'un des plus grands pays du monde dans le domaine de la cybersécurité, met en relief Ran Natanzon.

Il a également souligné que cette tendance renforcera la force du secteur de la recherche scientifique et du développement, qui représente en Israël 5,4% du produit intérieur brut (2021), sachant que la part par habitant du PIB s'est élevée au quatrième trimestre de 2021 à environ 44 mille 214 dollars.

Il ajoute que ce taux place Israël au premier rang mondial dans le domaine de la recherche et du développement, et au cinquième dans les technologies modernes (compte tenu de la population), tandis que la part des exportations israéliennes dans le domaine de la haute technologie a atteint environ 54% en 2021.

Quant à la part des employés dans le secteur de la haute technologie, elle s'élève à 10,4 % de la main-d'œuvre totale en 2021.

Afin de développer le centre de Beer-Sheva, la Direction du cyberespace d'Israël apporte son soutien aux entreprises qui s'installent dans la région.

Depuis la même ville, le centre de gestion des cyber-incidents gère le projet "Dôme de fer", qui vise en général à surveiller et à suivre diverses cyberattaques ciblant toutes les infrastructures en Israël.

Dans une déclaration à la MAP, le directeur exécutif de la politique et de la stratégie au département israélien de la cybersécurité, Roy Yarom a indiqué que le projet "Dôme de fer" fournira une protection complète des installations économiques et administratives, ainsi que des PC à même d'améliorer la défense du cyberespace israélien et renforcer sa structure de bouclier.

M. Yarom souligne, en outre, qu'Internet deviendra inévitablement l'une des dimensions de la guerre future, sinon la plus importante.

Il dit également que tout le monde devrait prendre la cybersécurité au sérieux car les cybercriminels ciblent non seulement les agences gouvernementales et les institutions privées, mais aussi les employés, les gens ordinaires et

même les enfants et les mineurs, les catégories les plus vulnérables de la société.

D'autre part, il a mis en avant qu'il existe des opportunités prometteuses de coopération entre le Maroc et Israël dans le domaine de la cybersécurité et du numérique pour un cyberespace ouvert, fiable, sécurisé et stable.

M. Yarom a mis en exergue les opportunités prometteuses de coopération dans les domaines académique et scientifique, la recherche et le développement, en plus de l'échange d'informations et de compétences, d'étudiants et l'organisation de recherches conjointes.

Il a également souligné l'importance d'améliorer ces échanges, afin de répondre aux menaces mondiales et d'asseoir des normes de comportement responsable dans le cyberespace.

Au vu du développement important du secteur de la cybersécurité en Israël, du nombre de transactions qu'il réalise et de l'attractivité croissante qu'il connaît à l'échelle mondiale, un rendez-vous international annuel régulier est organisé sous le nom de "Cyber Week", dont la dernière édition a été tenue à l'Université de Tel-Aviv en juin dernier, en coopération avec le ministère israélien des Affaires étrangères.

Cet événement international offre aux experts de l'industrie, du gouvernement, de la défense et du milieu universitaire l'occasion de partager leurs connaissances sur les défis et les opportunités dans ce domaine, de discuter des questions des cyberattaques, des dommages causés aux infrastructures vitales des pays, des dépenses publiques dédiées au secteur de l'informatique, des dépenses allouées à la cyber-protection et de la violation de la vie privée.

Selon les résultats de l'une des études présentées lors de la dernière édition de cette conférence, les dépenses de cybersécurité destinées à la protection des données et à la gestion des risques liés à l'informatique devraient atteindre 172 milliards de dollars dans le monde en 2022.

Une autre étude a rapporté que la cybercriminalité a considérablement augmenté pendant la pandémie de Covid-19, la fraude en ligne s'est accrue de plus de 400% en 2020 par rapport aux années précédentes et les messages frauduleux ont doublé de façon spectaculaire alors que Google a bloqué quotidiennement plus de 18 millions d'e-mails malveillants et d'hameçonnage durant la pandémie.

Cela comprend les escroqueries, le vol ainsi que l'implantation de logiciels de suivi malveillants et d'espionnage.

תיק עיתונות

יחסי ציבור (ישראל): אייזנברג אליאש

SPONSORS & PARTNERS

Distinguished Benefactor

THE SAGOL NETWORK

Diamond Sponsors

FORESCOUT

Esteemed Platinum Sponsors

CHECK POINT · IAI · Trellix · YL VENTURES

Platinum Sponsors

BAYER · HOLISTICYBER · IBM · Microsoft · SYGNIA · TEAM8

Gold Sponsors

Checkmarx · CYBERARK · CROWDSTRIKE · ermetic · intuit (turbotax, quickbooks, mint, credit karma, mailchimp) · MANDIANT · MITIGA · SIMSPACE · SYNOPSYS

Silver Sponsors

BioCatch · CYE · Elron Ventures · FORTINET · Google · NTT · NVIDIA · OUTSEER · Synamedia · TEAM CYMRU

Bronze Sponsors

Acronis · amdocs · cervello · CYLUS · cyviation · T · DoubleVerify · enav group · CYBER CONTROL · SOMPO Digital Lab Tel Aviv · TREND MICRO

Partners

U.S. Chamber of Commerce · Israel Innovation Authority · Israel Tech Policy Institute · המרכז לחינוך סייבר Cyber Education Center · CYBTOGETHER · Ministry of Energy www.energy.gov.il · BSIDES TLV 2022 · KONFIDAS · CSA Israel cloud security alliance · HiTech Ambassadors · CYTACTIC · UK Israel Tech HUB · Tel Aviv University · Embassy of the Federal Republic of Germany Tel Aviv · IATI · CAAI · קרן רש"י · משרד הביטחון Ministry of Defense · GLILOT · JETRO · DSI · conexx · BUSINESS FRANCE · OurCrowd · FUTURE OF PRIVACY FORUM · GOODWIN

כאן 11

"נקים כיפת ברזל טכנולוגית": ישראל מארחת את שבוע הסייבר העולמי

הארץ

מלחמת הסייבר בין ישראל לאיראן עלתה מדרגה והנזק שנגרם חמור מבעבר

לדברי ראש מערך הסייבר, בשנה האחרונה נבלמו כ-1,500 ניסיונות תקיפה, שחלקם בוצעו בידי גורמים איראניים. לצד זאת, בשבועות האחרונים נרשמו כמה ניסיונות מצד טהראן להוציא פיגועים כלפי ישראלים באיסטנבול, שסוכלו באמצעות שיתוף פעולה מבצעי הדוק עם הטורקים

עמוס הראל

נראה שמלחמת הסייבר בין ישראל לאיראן עלתה עוד מדרגה. השבוע דווח באיראן על מתקפת סייבר מסיבית, שפגעה קשות בתעשיית הפלדה במדינה. למתקפה קדמו ניסיונות איראניים חוזרים ונשנים לפגוע בתשתיות בישראל באמצעות תקיפות סייבר. ככל הידוע, בחלק מן התקיפות האחרונות נגד ישראל נגרם נזק חמור יותר מכפי שאירע בעבר. באחד המקרים, שעליו דווח בתקשורת, חדרו האקרים למערכות כריזה אזרחיות של כמה רשויות מקומיות וגרמו להפעלת צופרי התרעה.

בהקשר לכך, אמר אתמול (שלישי) ראש הממשלה, נפתלי בנט, בכינוס סייבר באוניברסיטת תל-אביב כי "כמו שיש הרתעה גרעינית, יש גם הרתעה בסייבר. בגישה שלי, בנוגע לאיראן, המדיניות שלנו היא שאם אתה מתעסק עם ישראל – אתה משלם מחיר. אם מישהו תוקף אותנו בסייבר, אנחנו נתקוף בחזרה".

בנט מרבה לדבר באחרונה על שינוי שנדרש במאזן ההרתעה מול איראן, ועל הצורך לפעול כנגד המשטר בטהראן, גם על אדמתו, בשלל תחומים שאינם מתמצים בתחום הגרעין. הוא סבור כי ישראל צריכה להרתיע את איראן גם באמצעות פגיעה בבכירים המעורבים בפעולות טרור ובחימוש ארגונים כמו חיזבאללה ובמקרה הצורך בעזרת תקיפות סייבר. בנט

ערך אתמול הערכות מצב וביקורי פרידה במטות של המוסד ושב"כ, לקראת העברת ראשות הממשלה ליאיר לפיד. הוא אמר כי אף שהמצב הפוליטי אינו יציב, "אסטרטגיית הביטחון הלאומי שלנו יציבה וברורה – יוזמה, הרתעה ובניין כוח".

באיראן דווח שלשום כי חברת חוזסטן, אחת מחברות הפלדה הגדולות במדינה, נאלצה להפסיק את הייצור במפעליה עקב מתקפת סייבר. המתקפה תוארה כאחת הגדולות מסוגה בתקופה האחרונה. ענף הפלדה הוא אחד הענפים הכלכליים המרכזיים באיראן ושיתוק המפעלים עשוי לארוך שבועות אחדים, עד לתיקון הנזקים. קבוצת האקרים נטלה אחריות לתקיפה – אותה קבוצה שבעבר קיבלה על עצמה אחריות לתקיפות נגד תחנות דלק ברחבי איראן. לאחר הפגיעה בתחנות הדלק, ייחסו גורמים איראניים את המהלך לישראל.

ראש מערך הסייבר הלאומי, גבי פורטנוי, אמר אתמול כי "איראן הפכה לשחקן מרכזי שאנחנו מזהים במרחב הסייבר, יחד עם חמאס וחיזבאללה". לדבריו, מערך הסייבר בלם בשנה האחרונה כ-1,500 ניסיונות תקיפה. "מגוון התוקפים בזירת הסייבר הורחב וכולל גם תוקפים נוספים – קבוצות תקיפה, שלוחות של מדינות, ארגוני פשיעה, אנשים פרטיים ועוד", אמר. פורטנוי הוסיף כי נדרשת "כיפת ברזל הגנתית בסייבר, שתגן על אזרחי ישראל ותצמצם את מתקפות הסייבר בצורה משמעותית".

תקיפות הסייבר האיראניות הן מימד נוסף שבו מתבטאת המתיחות עם ישראל. בחודשים אפריל ומאי נעשו כמה ניסיונות איראניים לפגוע בתיירים ישראלים בחו"ל. בסוף מאי נהרג קולונל במשמרות המהפכה, חסן סיאד חודאיארי, בפעולת התנקשות בטהראן. המתנקשים נמלטו. גם פעולה זו יוחסה באיראן לישראל, ואחריה הוגברו עוד יותר הניסיונות לפגוע בתיירים ישראלים על אדמת טורקיה.

בשבועות האחרונים הצליחו שירותי המודיעין של ישראל וטורקיה לשבש כמה מהניסיונות הללו, שהתמקדו בעיר איסטנבול. כמה חוליות ששלחו האיראנים נעצרו בידי הטורקים. אתמול הוחלט במטה ללוחמה בטרור להוריד את אזהרת המסע לישראלים מפני ביקור באיסטנבול מהרמה הגבוהה ביותר (רמה 4) לרמת סיכון בינונית (3), כמו בשאר חלקי טורקיה.

ראש חטיבת המודיעין במטה לביטחון לאומי, יוסי אדלר, אמר כי השינוי התאפשר הודות לשיתוף פעולה מבצעי ומודיעיני הדוק עם הטורקים, שהביא לסיכול הפיגועים. הוא הוסיף כי הורדת אזהרת המסע אינה פרוצדורה טכנית, אלא תוצאה של הערכת מצב המסתמכת על ניתוח הסיכונים. בנט הודה אתמול לנשיא טורקיה, רג>פ טייפ ארדואן, על הסיוע בסיכול הפיגועים.

כלכליסט

בנט: "צריך הרתעת סייבר - אם איראן תתקוף את ישראל, תהיה תגובת נגד"

ראש הממשלה היוצא אמר את הדברים בכנס שהתקיים במסגרת אירועי שבוע הסייבר באוניברסיטת תל אביב. כמו שיש הרתעה גרעינית, אני חושב שצריך לייצר גם הרתעת סייבר", הוסיף בנט ויעץ למנכ"לים שנכחו בכנס, בקריצה, שלא להיכנס לפוליטיקה

רפאל קאהאן

ראש הממשלה היוצא נפתלי בנט הגיע היום לאירועי שבוע הסייבר שמתקיים באוניברסיטת תל אביב בימים אלה וערך שיחה עם מיכל ברוורמן-בלומנשטיק, שותפתו לשעבר בחברת הסייבר סיוטה שנרכשה בזמנו על ידי מיקרוספט. בלומנשטיק-ברוורמן מכהנת כיום כמנכ"לית מרכז המחקר והפיתוח של מיקרוסופט בישראל וכסמנכ"לית הטכנולוגיה העולמית לאבטחת ענן ו־AI של החברה.

בשיחתה עם ראש הממשלה הדגישו השניים את החשיבות שיש לשיתופי פעולה בתחום הסייבר וכן התייחסו לאתגרי הסייבר הרבים כיום מול מדינות ולמחסור האקוטי של עובדים בתחום. בפתח דבריו התייחס ראש הממשלה למצב הפוליטי הנוכחי.

"העברנו את התקציב וביצענו רפורמות, אנחנו במצב של תעסוקה מלאה ושל 8% צמיחה – הגדולה ביותר בעולם המערבי. הביטחון חזר לדרום וילדי אשקלון ושדרות חיים בשקט. בשנה הזו עשינו 10 שנות עבודה והוכחנו לעצמנו ולמדינה שאנשים עם דעות פוליטיות שונות יכולים לעבוד ביחד. חילונים, דתיים, ימנים או שמאלנים - כולם יכולים לעבוד ביחד. זו היתה שנה די מדהימה".

ברוורמן-בלומנשטיק: סייבר הוא החזית של הלוחמה המודרנית - כיצד אתה רואה את המצב והאם ישראל מוכנה לאיומים האלה?

"כשמסתכלים על ההחזר על ההשקעה, כיום אפשר ללכת למבצעים שבעבר דרשו יחידות קומנדו רבות, תוך שימוש במישהו מאחורי מקלדת. הופתעתי שסייבר לא שומש בצורה הרבה יותר מסיבית במלחמה באוקראינה. מה שבטוח זה שבשנים הקרובות אנחנו נראה השקעות גדולות בכל העולם בסייבר התקפי - וכמובן שזה גם מתחבר לפשע. אם אתה יכול לפעול ביעילות בלי לחשוף את עצמך, מדובר בדרך מצוינת עבורם לפעול".

בנט גם התייחס למצב הנוכחי בישראל. מערך הסייבר הלאומי הוא הזרוע העיקרית של המדינה בכל הנוגע לנושאי סייבר אזרחיים ובנט התגאה בקידום של הארגון החוסה תחת משרד ראש הממשלה. "מיניתי ראש חדש למערך הסייבר – גבי פורטנוי – אבל החברות אחראיות בעצמן להגנת סייבר. כעת, הקבוצה של פורטנוי עובדת עם המשק ועם החברות כדי לקדם את הנושא. אמנם המצב לא מושלם אבל הוא משתפר".

בנוגע למלחמת הסייבר החשאית שמתקיימת בין איראן לישראל, אמר בנט: "כמו שיש הרתעה גרעינית, אני חושב שצריך לייצר גם הרתעת סייבר. הרעיון הוא שאם איראן תתקוף את ישראל – תהיה תגובת נגד. אתה לא תוכל לשלוח את סוכניך - חיזבאללה או חמאס - ולא לצפות לתגובה. לא נאפשר פגיעה ללא תגובה. מעבר לכך אנחנו מקדמים שיתופי פעולה כי היום מדובר בחיבור בין החברות והמדינות. אם מצביעים על העבריין, כולם יכולים להילחם נגדו. אנחנו עובדים עם שותפינו באירופה ובארה"ב כדי לקדם זאת".

ברוורמן-בלומנשטיק : זאת בהחלט מלחמה שניתן לנצח בה אם נעבוד ביחד. אנחנו משתפים מידע בינינו לבין עצמנו (ענקיות הטכנולוגיה אפל, גוגל, מיקרוסופט ואחרות, ר>>ק), וגם עם ממשלות.

"צריך לשלב את השת>>פ הזה בקואליציה ואולי תהיה לנו מדינה יותר יציבה", התלוצץ ראש הממשלה בתגובה.

ברוורמן-בלומנשטיק: אנחנו חייבים יותר אנשים בתעשייה – כיצד עושים זאת?

"בישראל יש לנו הרבה מאוד השקעות, אבל אנחנו צריכים אנשים טובים נוספים. יש לנו ארבעה מקורות נוספים לכוח אדם: חרדים – הם חכמים מאוד, אבל צריך ללמד אותם אנגלית ולקדם אותם במקצועות כגון מתמטיקה; נשים ערביות - מה שדורש גם פתיחות מצד התעשיה; הפריפריה – מצחיק לקרוא כך למקומות שנמצאים 40 דקות מהמרכז, בעיקר אם אתה משווה למדינות כמו הודו או ארה"ב, אבל מדובר במקומות שלא מונגשים וכעת אנחנו מנסים, דרך הצבא, לפתוח שלוחה של יחידה 8200 שתגייס תלמידים במקומות האלה ; ושילוב של פלסטינים בתעשייה דרך שיתופי פעולה עם הרשות הפלסטינית. אנחנו יכולים לקדם תנופת גיוס חדשה.

ברוורמן-בלומנשטיק: מיקרוסופט עובדת עם חרדים שעברו לימודי ליב>>ה. ההייטק לא יוכל שרוד ללא שילוב של אנשים שאינם מהמרכז.

בנט: "יש גם את הישראלים שעובדים בחו>>ל. אני קורא להם: בואו הביתה. זו מדינה נהדרת"

ברוורמן-בלומנשטיק: מה התובנות שתוכל לשתף עם כל המנכ>>לים כאן במליאה?

"מנכ>>לים וראשי ממשלה זה שונה, אבל השיעור הגדול זה לזוז מהר. בפוליטיקה אתה לא יודע מה האופק ואתה חייב לזוז מהר. עסקים ופוליטיקה פועלים בצורה כמעט הפוכה, אבל כשאתה אומר וקובע מדיניות, אתה חייב לבצע אותה. כמו כן, אתה חייב לעקוף את ההיררכיה, לדבר עם האנשים למטה ישירות. והעצה הכי חשובה שלי למנכ>>לים: אל תיכנסו לפוליטיקה. מה שחשוב זה שכולנו נעבוד ביחד כדי להילחם באנשים הרעים ואני מאוד אופטימי לגבי זה".

הארץ

ראש מערך הסייבר: מתחילת השנה בלמנו 1,500 ניסיונות תקיפה של העורף

לדברי ראש המערך פורטנוי, איראן היא שחקנית מרכזית במרחב הסייבר, לצד חמאס וחיזבאללה. הוא הוסיף כי המערך שבראשותו עוסק בימים אלה במציאת פתרון להגנה כוללת על המשק

מערך הסייבר הלאומי בלם מתחילת השנה כ-1,500 נסיונות תקיפה של העורף, כך אמר היום (שלישי) ראש המערך גבי פורטנוי. לדבריו, איראן היא שחקנית מרכזית במרחב הסייבר, לצד חמאס וחיזבאללה. "אנחנו רואים אותם, אנחנו יודעים איך הם עובדים ואנחנו שם", אמר פורטנוי.

ראש המערך, שאמר את הדברים בכנס הסייבר הבינלאומי באוניברסיטת תל אביב, הוסיף כי הוא עוסק בימים אלה במציאת פתרונות למתן הגנה כוללת למשק. "אנחנו צריכים כיפת ברזל הגנתית בתחום הסייבר לטובת אזרחי ישראל", אמר. "כיפת הסייבר היא פרויקט הדגל החדש שלנו במערך לחיזוק ההגנה של המשק כולו".

לדבריו, המערך שבראשותו עובר "מפרדיגמה שמסתכלת על התוקף לפרדיגמה שמסתכלת על העורף האזרחי". כמו כן, הוא ציין שאנשיו החלו להסתכל על המשק באופן מגזרי, "הסתכלות על פי תחומים ולא על פי גופים". בהתייחס לסוגי התוקפים הוא אמר כי לצד גורמים מדינתיים, במערך מזהים "תוקפים נוספים - קבוצות תקיפה, שלוחות של מדינות, ארגוני פשיעה, אנשים פרטיים ועוד".

בשבוע שעבר הופעלו צופרים בירושלים ובאילת, ומערך הסייבר חושד שמקורן של האזעקות הוא במתקפת סייבר על ממשק מערכות הכריזה. במערך בודקים אם איראן היא שעומדת מאחורי התקיפה. בנוסף, באחרונה פרסמה חברת צ>ק פוינט דו"ח על מבצע ריגול איראני שבמסגרתו השתלטו האקרים על חשבונות מייל של בכירים ישראלים והתחזו אליהם.

ישראל היום
הכי ישראלי כל הזמן

בנט על איראן: "אם הבריון שולח אנשים להכות אותנו - נכה אותו בכל הממדים"

ראש הממשלה התראיין בכנס הסייבר באוניברסיטת תל אביב • "הסייבר הוא חזית הלוחמה המודרנית, פעולות שבעבר היו דורשות 100-50 לוחמים מאחורי קווי האויב, אפשר לבצע היום עם אנשים חכמים שיושבים מאחורי מקלדת" • על ימיה האחרונים של הממשלה אמר: "הוכחנו שאפילו דעות מנוגדות יכולות לעבוד ביחד"

תמיר מורג, אריאל כהנא

"הגישה שלי לאויבינו, במיוחד לאיראן, היא שלא נמיט עליהם הרס, אבל מי שיתעסק עם ישראל ישלם מחיר, הסייבר הוא חזית הלוחמה המודרנית".

ראש הממשלה, נפתלי בנט, השתתף היום (שלישי) בכנס לכבוד שבוע הסייבר באוניברסיטת ת"א. במהלך הריאיון הוא נשאל כיצד הוא רואה את ההתקדמות של ישראל בתחום הסייבר ומהם האיומים שישראל מתמודדת איתם.

בתגובה, ענה ראש הממשלה: "מנקודת התצפית של ראש הממשלה חשבנו על תהליך קבלת החלטות עבור כל מנהיג שנמצא במלחמה. היום אתה יכול לפגוע באויב שלך באמצעות סייבר, שבעבר היה דורש 100-50 לוחמים מאחורי קווי האויב תוך סיכון עצום. עכשיו חבורה של אנשים חכמים שיושבים ליד מקלדת יכולים להשיג את אותו הדבר.

"באופן בלתי נמנע הסייבר הולך להפוך לאחד הממדים הבולטים ביותר של לוחמה עתידית. כמו שיש הרתעה גרעינית, תהיה גם הרתעה בסייבר. קצת הופתעתי מהמחסור בכלי סייבר במלחמה באוקראינה, חשבתי שזה יהיה הרבה יותר מתקדם והרבה יותר מסיבי. בצד ההגנתי, אני לא רוצה להגיד שהכל מושלם, אבל סך הכל מצבנו די טוב. אי אפשר יותר לפגוע בישראל דרך צד שלישי ולהתחמק מזה".

כמו כן, בנט טען כי אם תאותגר ביטחונית, ישראל תתקוף ישירות את איראן - לא רק בסייבר אלא גם בפצצות ("אמצעים קינטיים"), זאת בניגוד למדיניות של לתקוף את שליחיה של איראן. "הגישה שלי לאויבינו, במיוחד לאיראן, היא שלא נמיט הרס, אבל אם תתעסקו עם ישראל תשלמו מחיר. אם הבריון שולח אנשים להכות אותנו, אנחנו הולכים להכות את הבריון בכל הממדים. אם מישהו יתקוף אותנו בסייבר, אנחנו נתקוף בחזרה" אמר.

יתר על כן, בנט דיבר על אחריותם של תאגידי הענק לדעת להתמודד עם מתקפות זרות שמסכנות את הלקוחות שלהם. "בסופו של יום, תאגידים צריכים לקבל אחריות וכשהם מתעסקים בנתוני הלקוחות שלהם זו הבעיה שלהם, אבל זה לא מספיק. ברמה הלאומית - מערך הסייבר בראשות פורטנוי עובד עם החברות כדי לעזור להן להגן על עצמן, עם התשתיות הקריטיות. אנחנו מצליחים די טוב בצד ההגנתי ובממד הצבאי".

כמו כן, באשר לשאלת פיתוח האקוסיסטם של הסייבר בארץ, אמר ראש הממשלה: "אני רואה ארבע קבוצות שונות של כישרונות חדשים בתחום ההייטק והסייבר, שאותן אנחנו צריכים להבין כיצד משלבים - חרדים, נשים ערביות, אנשים מהפריפריה ואף פלשתינים. נתתי אישור להצטרפות מיידית של עובדים פלשתינים להייטק הישראלי, כולל אישורי תנועה לבוא לכאן".

מסכם שנה כראש ממשלה

פרט לדיבורים על עתיד הסייבר הישראלי, בנט ניצל את ההזדמנות גם כדי לסכם את שנתו כראש ממשלת ישראל ואת הישגי הקואליציה. "בחזית הדרום זו הייתה השנה השקטה ביותר זה 50 שנה. בשנה אחת עשינו 10 שנים של עבודה. הוכחנו שאפילו דעות מנוגדות יכולות לעבוד ביחד. כשיש אנשים הגונים וטובים, נוכל לעבוד יחד על שיפורה של ישראל.

"הייתי פה לפני שנה, וישראל הייתה אחרי בחירות בבלאגן: בלי תקציב, והמדינה עדיין ליקקה את פצעיה אחרי מהומות שהיו לנו. התחלנו לנהל את המדינה כמו שצריך לנהל, חבורה של שרים שמנסים לעשות את הטוב ביותר עבור המדינה. העברנו תקציב אחרי 3 שנים, ירשנו שיעור אבטלה גבוה מאוד ועכשיו אנחנו בתעסוקה מלאה. יש לנו צמיחה של 8% - הגבוהה ביותר בעולם המתקדם. אני לא מרוצה מהבחירות, זה בהחלט לא טוב לישראל. הוכחנו שמי ששומר על דעות מנוגדות יכול לעבוד היטב יחד לטובת מדינה".

מעריב

"איראן הפכה לשחקן מרכזי": כמות תקיפות הסייבר שנבלמו השנה נחשפת

בנאומו הראשון מאז כניסתו לתפקיד, אמר ראש מערך הסייבר הלאומי כי נמנעו מספר רב של תקיפות. וציין כי "איראן הפכה לשחקן מרכזי שאנו מזהים במרחב הסייבר"

סתיו נמר

ראש מערך הסייבר הלאומי, גבי פורטנוי, חשף היום (שלישי) בשנה האחרונה בלם המערך כ-1,500 נסיונות תקיפה שונים על העורף הישראלי. את הדברים אמר בנאום מקיף ראשון מאז כניסתו לתפקיד לפני כארבעה חודשים, במסגרת שבוע הסייבר השנתי בהובלת המרכז למחקר סייבר באוניברסיטת ת"א, מערך הסייבר הלאומי, משרד הכלכלה ומשרד החוץ. לדברי פורטנוי בכנס, "למערך יש נקודת תצפית ייחודית על ההגנה המדינתית. אנחנו עוברים להסתכלות מגזרית על המשק – הסתכלות על פי תחומים ולא על פי גופים. אנחנו עוברים מפרדיגמה שמסתכלת על התוקף לפרדיגמה שמסתכלת על העורף האזרחי". בהתייחס לסוגי התוקפים אמר, "מגוון התוקפים בזירת הסייבר הורחב וכולל גם תוקפים נוספים, קבוצות תקיפה, שלוחות של מדינות, ארגוני פשיעה, אנשים פרטיים ועוד. איראן הפכה לשחקן מרכזי שאנו מזהים במרחב הסייבר, יחד עם חמאס וחיזבאללה. אנחנו רואים אותם, אנחנו יודעים איך הם עובדים ואנחנו שם".

בהמשך, הציג אש מערך הסייבר הלאומי את הפרויקט החדש של המערך ליצירת כיפת סייבר על המרחב האזרחי. "כיפת הסייבר היא פרויקט הדגל החדש שלנו במערך לחיזוק הגנת הסייבר של המשק כולו. הפרויקט יעשה שימוש במנגנונים חדשים ויביא לצמצום מתקפות הסייבר בצורה משמעותית. כיפת הסייבר היא גישה פרו-אקטיבית חדשה לחיזוי ובלימת מתקפות שמשלבת טכנולוגיות של ביג-דאטא ובינה מלאכותית", הסביר.פורטנוי הציג את ההרחבה של הכלים של המערך ופתיחתם מהטמעה בתשתיות הקריטיות בלבד לסקטורים ותחומים נוספים. לסיכום אמר כי "רק באמצעות שיתוף פעולה – בין מדינות, עם חברות הגנת הסייבר, האקדמיה, הממשל וגופי הבטחון - נוכל להגן על עצמנו במלחמת הסייבר וליצור כיפת ברזל הגנתית בסייבר רחבה".

ישראל היום
הכי ישראלי כל הזמן

גנץ חשף: "איראן וחיזבאללה פעלו יחד כדי לפגוע בפעילות יוניפ"ל בלבנון"

שר הביטחון השתתף בכנס הסייבר הבינלאומי באוניברסיטת תל אביב וטען כי "ישראל מכירה את מערכות הסייבר של יריביה ואת דרכי הפעולה שלהם • גנץ התייחס בין היתר לתיעוד של אל-סייד בשבי החמאס: "סרטון שמטרתו סחטנות – על גבה של סוגייה הומניטארית" • סגן מפקד יחידת 8200 חשף: "סיכלנו את הניסיון להרעיל את מערכות המים

לילך שובל

שר הביטחון, בני גנץ נאם הבוקר (רביעי) בכנס הסייבר הבינלאומי של מרכז הסייבר באוניברסיטת ת"א ושם חשף מתקפה משותפת של איראן וחיזבאללה בכדי לפגוע בכוחות יוניפ"יל בלבנון, "פגיעה נוספת של איראן וחיזבאללה באזרחי לבנון ויציבות המדינה", אמר גנץ.

גנץ התייחס בין היתר לתיעוד של הישאם אל-סייד, השבוי בשבי החמאס בעזה, אותו שיחררה הזרוע הצבאית של ארגון הטרור: "אתמול פורסם סרטון שמטרתו סחטנות – על גבה של סוגייה הומניטארית. חמאס מחזיק בשבי את ארבעת הבנים בניגוד לחוק הבינלאומי, בניגוד למוסר. חמאס אחראית לכך והציפייה שלנו מהקהילה הבינלאומית היא לפעול מול ההתנהלות הנפשעת הזו של חמאס".

עוד הוסיף כי "מדינת ישראל פועלת במגוון אמצעים, וממשיכה להפוך כל אבן על מנת להשיב את הבנים הביתה. כפי שאמרנו בעבר – מדובר בסוגיה הומניטארית, כך אנו רואים אותה, ועל הבסיס הזה נמשיך לפעול. ניסיונות סחטנות ותרגילי תודעה לא ישפיעו על עמדתנו והתנהלותנו".

בהמשך חשף פעילות משותפת של איראן וחיזבאללה: "איראן מפעילה את שלוחיה גם במימד הסייבר: אני יכול לחשוף היום, שלאחרונה אותרה פעילות של גופי הביטחון האיראנים בשיתוף עם חיזבאללה, בכדי לפגוע בפעילות כוחות יוניפי"ל בלבנון. זאת על ידי מימוש מבצע בסייבר שמטרתו הייתה לגנוב חומרים על היערכות יוניפ"ל במרחב, ושימוש

בהם על ידי חיזבאללה. זוהי פגיעה נוספת של איראן וחיזבאללה באזרחי לבנון, וביציבותה של לבנון".

"ישראל מכירה את מערכות הסייבר של יריביה ואת דרכי הפעולה שלהם. אנו רואים בשנים האחרונות תופעה של קבוצות האקרים מטעם איראן, שפועלות מול ישראל ומדינות נוספות", המשיך גנץ וסיפר. "<השלוחים החדשים>, הם טרוריסטים עם מקלדת שדינם כמו לוחמי ארגוני טרור אחרים. אנחנו יודעים מי הם, אנחנו פוגעים בהם ובשולחיהם, וגם היום הם על הכוונת שלנו – ולא רק במימד הקיברנטי. שום מתקפה מול אזרחי ישראל לא תעבור לסדר היום. והאחריות היא של התוקפים ושל המדינה שממנת ושולחת אותם. תקיפת סייבר יכולה להיענות במגוון דרכים במרחב הסייבר ובמרחבים נוספים".

גנץ המשיך במתקפה על מעצמת הגרעין: "איראן מובילה את טרור הסייבר – ועושה מהלכים שמטרתם להשפיע על תהליכים דמוקרטיים ועל ממשלים, כפי שקרה בבחירות לנשיאות ארצות הברית ובניסיונות נוספים שישראל מודעת אליהם. פעולות כמו זו של יחידת <שאהיד כאווה> שאספה מידע על ספינות, תחנות דלק ומפעלי תעשייה במספר מדינות, נעשו תחת דירקטיבה ישירה של ההנהגה האיראנית ומשמרות המהפכה כפי שנחשף בתחקירים".

עוד הוסיף כי "בשנים האחרונות בלמנו ניסיונות רבים לפרוץ לחברות פרטיות וציבוריות, בארץ ובחו"ל. אני קורא גם לציבור לדרוש <אחריות קיברנטית>, ולהעניש חברות וגופים שלא פועלים בהתאם להנחיות".

גנץ המשיך וסימן את היעדים הבאים של ישראל מול האיומים: "המשימה העליונה שלנו, בצבא, בתעשיות ובארגוני הביטחון השונים היא לבנות את האנשים, להכשיר אותם, ולהשאיר אותם. אני והרמטכ"ל הצבנו את הנושא הזה כאחת המשימות המרכזיות ביחידות הרלבנטיות. אנחנו בוחנים את בניין הכוח כל העת – גם בהיקפי כוח האדם, גם בנושא ההכשרות וגם בנושא המשימות. בשנים הקרובות נצטרך גם לבחון את צורת ההתארגנות, הניהול והתפעול של לוחמת הסייבר, על מאפייניה ההתקפיים וההגנתיים בצה"ל ובמערכת הביטחון כולה".

לבסוף סיכם שר הביטחון וקרא לשיתופי פעולה עם העולם: "יש חשיבות גדולה לשיתופי הפעולה שלנו עם העולם מול איראן גם במימד הסייבר. את אותם שיתופי פעולה שאנו בונים באזור מול איראן בהיבטים של הגנה מול איומים שונים – אנחנו מרחיבים גם במימד הסייבר".

סגן מפקד יחידת 8200 חשף: "סיכלנו את הניסיון להרעיל את מערכות המים"

אורי, סגן מפקד יחידת 8200, אמר בהופעה הפומבית הראשונה של היחידה בכנסים מסוג זה, חשף כי ישראל סיכלה התקפה על מערכות המים.

"סיכול איומי סייבר הוא חלק מרכזי בפעילות שלנו. מטרתנו להשיג עליונות על התוקף, להצליח לזהות אותו ולפעול כדי לשלול את יכולותיו". אמר סגן מפקד 8200 והוסיף "כך לעיתים אנו גם מוצאים קורבנות מחוץ לישראל ואז אנו יוצרים קשר עם סוכניות אחרות אם צריך. אנו עושים זאת גם באופן עצמאי וגם על ידי שיתוף פעולה עם התעשייה וסוכנויות אחרות, באמצעות יישום ושימוש בכלים שפיתחנו. 8200 לא תנוח עד שהאיום יוסר".

כאמור, כך נחשף איום על מערכות המים של ישראל והניסיונות להרעיל את אזרחי ישראל: "סיכלנו את הניסיון להשתלט על מערכות המים הקריטיות של ישראל ולהרעיל אותן לפני מספר שנים. במקרה אחר זיהינו גם כי יריב מסוים תקף את ישראל ותוך כדי זיהינו שאותו תוקף ניסה גם לכוון לתחנות כוח בארה"ב. זו הייתה האינדיקציה הראשונה להתקפה זו. את האיום הזה הצלחנו למנוע באמצעות שיתוף פעולה הדוק עם השותפים האמריקאים שלנו".

מעריב

ראש הממשלה בנט במסר לאיראן: "מי שיתקוף אותנו דרך סייבר - נתקוף בחזרה"

ראש הממשלה היוצא, נפתלי בנט, השתתף בכנס הסייבר העולמי באוניברסיטת תל אביב והתייחס לאיומי הסייבר על ישראל מצד איראן: "אי אפשר כבר לפגוע בנו בעקיפין ולא לשלם על זה"

רגע לפני סיום כהונתו: ראש הממשלה, נפתלי בנט השתתף היום (שלישי) בכנס הסייבר העולמי באוניברסיטת תל אביב, והתייחס לאיומי הסייבר על ישראל מצד איראן, דרך הפעולה של ישראל בנידון, וכן כיצד מעוניין להכניס עוד קבוצות בחברה הישראלית להייטק."הייתי מופתע מחוסר השימוש בכלי הסייבר במלחמה באוקראינה", אמר רה"מ בנט בפתח דבריו, "חשבתי שזה יהיה שימוש מתקדם יותר וזה לא קרה. אם אפשר להשיג את אפקט המלחמה דרך הסייבר ולא לסכן חיי אדם, זה מה שצריך לעשות ברמה הפוליטית - נראה הרבה התקדמות ברחבי העולם בתחום הסייבר ההתקפי מן הסתם, זה תקף גם על פשע."הגישה שלי בנושא איראן זה לא רק לייצר כאוס בטהרן, אלא זה שיש מחיר להתעסקות עם ישראל ואי אפשר כבר לפגוע בנו בעקיפין דרך פרוקסי כמו חיזבאללה וחמאס ולא לשלם על זה", הוסיף, "אם אתה הבריון ששולח שליחים אלינו, אנחנו לא נכה אותם, אלא את הבריון וזה תקף בכל החזיתות. אם מישהו יתקוף אותנו דרך סייבר נתקוף בחזרה".

"האנשים הרעים שתוקפים חברה או מדינה יתקפו גם אחרים. אם נוכל לשתף את המידע הזה ולספר לכולם מי הבריון שתוקף, אז כל המדינות יוכלו להגן על עצמם מפניו. מה שאנחנו עושים זה להגדיל את הרשת הגלובלית, עובדים עם ארה"ב, בריטניה, צרפת וזה חיוני ונמשיך עם זה. הייתי מביא את שיתוף הפעולה מהייטק לקואליציה, אולי הייתה יותר יציבות לממשלה ולישראל", ציין רה"מ בנט.

לאחר מכן התייחס לקבוצות בחברה ישראלית ואמר כי "החרדים הם אנשים מאוד חכמים אבל הם לא בתוך עולם הכלכלה. הגישה בעשור האחרון הייתה לא פופולרית אבל זו עכשיו מדיניות של כולם - לעשות את הדבר החכם ולהשקיע בחרדים ולעזור להם להצטרף לכוח העבודה בגיל צעיר, כי להתגייס הם לא יתגייסו. זה מאתגר כי החרדים לא לומדים אנגלית וצריך ללמד אותם. התחלנו עכשיו תוכנית לחכמים ביותר בתלמידי החרדים, הם לומדים אנגלית ומתמטיקה ואני אופטימי."קבוצה נוספת - נשים ערביות", אמר בנט, "הן חלק קטן מכוח העבודה, אנחנו רוצים להגדיל את הנוכחות שלהן בהייטק ועובדים על זה. אנחנו רוצים להביא להייטק אנשים שונים, אנשים שהם לא מי שהיו בהייטק עד עכשיו. יש החלטת ממשלה מיידית לצרף עובדים פלסטינאים להייטק הישראלי כולל תנועה חופשית משטחי הרשות לכאן, אנחנו בודקים איך זה יעבוד".לסיום אמר: "הפריפריה של ישראל היא 40 דקות מתל אביב, זה מצחיק להגיד את זה לארה"ב או הודו, אבל זו האמת. זה לא חודש נסיעה כמו במדינות אחרות. אבל במשך הרבה שנים, הגליל והנגב היו מקופחים בגלל מדיניות טיפשית של ישראל".בתחילת השבוע, נפרד בנט מהשרים בישיבת הממשלה: "אף פעם לא שמעתי מישהו דואג למגזר שלו או למפלגה שלו, והייתה ממשלה מצוינת. ידענו להניח בצד מחלוקות אידאולוגיות ולפעול. יש ממשלות ארוכות שנים עם הישגים דלים מאוד, אנחנו ממשלה קצרת שנים עם הישגים אדירים".

ynet
ידיעות אחרונות

בנט: "מה שדרש פעם עשרות אנשי קומנדו - מצריך כמה אנשים ומקלדת"

ראש הממשלה נפתלי בנט אמר בכנס לרגל שבוע הסייבר השנתי באוניברסיטת תל אביב, כי: "היום אפשר לעשות דברים - פגיעה באויב, דרך הסייבר. מה שבעבר דרש שליחת 50-100 אנשים קומנדו בסודיות מאחורי קווי האויב דורש היום כמה אנשים ומקלדת. בסופו של דבר הסייבר יהפוך למרחב הכי בולט של לחימה בעתיד". הוא הוסיף: "אני די מופתע מהמחסור או המחסור היחסי של כלי סייבר מסיביים במלחמה באוקראינה. בראש ובראשונה ברמה הגיאו-פוליטית נראה המון השקעות ברחבי העולם בהתקפות סייבר".

ynet
ידיעות אחרונות

ynet
ידיעות אחרונות

גנץ חשף: "איראן וחיזבאללה ניסו לפגוע בפעילות יוניפי"ל בלבנון"

לפי שר הביטחון, מטרתם הייתה לגנוב חומרים על היערכות יוניפי"ל, שבהם רצה חיזבאללה להשתמש. בכוח הצבאי של האו"ם גילו על כך מנאום גנץ: "לא קיבלנו מידע ישיר". על הסרטון של הישאם א-סייד אמר: "תרגילי תודעה לא ישפיעו עלינו". סגן מפקד 8200 חשף: "סיכלנו ניסיונות השתלטות על מערכות המים הקריטיות של ישראל"

נינה פוקס, יואב זיתון

לאחר שבתחילת השבוע רמז על שיתוף הפעולה עם מדינות האזור נגד טהרן, על רקע הדיווח שלפיו הרמטכ"ל אביב כוכבי לקח חלק בדיון חשאי במצרים עם הרמטכ"ל הסעודי, חשף היום (רביעי) שר הביטחון בני גנץ שגורמי ביטחון איראנים, בשיתוף חיזבאללה, ניסו לפגוע בכוחות יוניפי"ל בלבנון. ynet העביר את הדברים בשידור ישיר.

לדבריו, איראן וחיזבאללה ניסו לעשות זאת באמצעות סייבר, ומטרתם הייתה לגנוב חומרים על היערכות יוניפי"ל במרחב, בהם תכננו בחיזבאללה לעשות שימוש. "זוהי פגיעה נוספת של איראן וחיזבאללה באזרחי לבנון וביציבותה", אמר גנץ.

"אנחנו רואים בשנים האחרונות תופעה של קבוצות האקרים מטעם איראן, שפועלות מול ישראל ומדינות נוספות", הוסיף גנץ. "<השלוחים החדשים> הם טרוריסטים עם מקלדת, שדינם כמו לוחמי ארגוני טרור אחרים. אנחנו יודעים מי הם, ואנחנו פוגעים בהם ובשולחיהם".

גנץ סבור שאיראן מובילה את טרור הסייבר, ועושה מהלכים שמטרתם להשפיע על תהליכים דמוקרטיים במדינות אחרות. "כפי שקרה בבחירות לנשיאות ארה"ב ובניסיונות נוספים שישראל מודעת אליהם. פעולות כמו של יחידת "שאהיד כאווה", שאספה מידע על ספינות, תחנות דלק ומפעלי תעשייה במספר מדינות – נעשו תחת הנחייה ישירה של ההנהגה האיראנית ומשמרות המהפכה, כפי שנחשף בתחקירים", אמר השר.

גנץ הוסיף כי "בשנים האחרונות בלמנו ניסיונות רבים לפרוץ לחברות פרטיות וציבוריות, בארץ ובחו"ל. אני קורא גם לציבור לדרוש <אחריות קיברנטית>, ולהעניש חברות וגופים שלא פועלים בהתאם להנחיות".

בכוח הצבאי של האו"ם, יוניפי"ל, לא הכירו את ניסיונות הפגיעה בכוחותיו וציינו כי זו הפעם הראשונה ששמעו על כך. "יוניפיל והאו"ם לוקחים ברצינות רבה את אבטחת הסייבר ויש להם אמצעים חזקים כדי להתגונן מפני התקפות. אנו מודעים לדיווחים על דבריו של שר הביטחון הישראלי גנץ, אך לא קיבלנו מידע ישיר על התקרית לכאורה", מסרו ביוניפי"ל לרויטרס.

גנץ התייחס לתיעוד שפרסם החמאס אתמול, שבו נראה השבוי הישראלי הישאם א-סייד כשהוא מחובר למכונת חמצן. גנץ אמר שמטרת פרסום הסרטון הייתה "סחטנות על גבה של סוגיה הומינטרית. ניסיונות הסחטנות ותרגילי התודעה לא ישפיעו על התנהלותנו. חמאס מחזיק את ארבעת הבנים בניגוד לחוק הבינלאומי ולמוסר. הציפייה שלנו מהקהילה הבינלאומית היא לפעול מול הפעילות הנפשעת הזו של חמאס". גנץ הוסיף כי "מדינת ישראל ממשיכה להפוך כל אבן על מנת להשיב את הבנים הביתה".

סגן מפקד יחידת 8200, שהשתתף גם הוא בכנס תחת השם "אורי", אמר כי צה"ל סיכל "ניסיונות השתלטות על מערכות המים הקריטיות של ישראל, שאותם ניסו להרעיל לפני מספר שנים. אותו אויב מסוים תקף את ישראל, ותוך כדי זיהינו שהוא מנסה לתקוף גם תחנות כוח בארה"ב". הוא הוסיף כי "את האיום הזה הצלחנו למנוע באמצעות שיתוף פעולה הדוק עם השותפים האמריקאים שלנו. הישגים כאלו הם שגורמים לחיילים שלנו להיות גאים בעבודתם ב-8200".

ראש הממשלה נפתלי בנט, שהשתתף גם הוא בשבוע הסייבר השנתי באוניברסיטת תל אביב, אמר אתמול כי "היום אפשר לפגוע באויב דרך הסייבר. מה שדרש בעבר 50-100 אנשי קומנדו שיפעלו בסודיות מאחורי קווי האויב, בסיכון גדול, אפשר להשיג היום באמצעות כמה אנשים חכמים שיושבים עם מקלדת".

הוא התייחס גם למתקפות הסייבר על תשתיות אזרחיות, ואמר כי לישראל יש הגנה טובה - אך "בסוף היום לתאגידים יש אחריות עצמית שהם חייבים לקחת על עצמם. אם נפרץ המידע של הלקוחות שלהם, זו בעיה שלהם. ברמה הלאומית, מערך הגנת הסייבר של ישראל עובד מול החברות כדי לעזור להן להגן על עצמן. זו תשתית קריטית". בנט הוסיף: "כמו שיש הרתעה גרעינית, תהיה הרתעת סייבר".

את הדברים אמר בנט קצת יותר מיממה לאחר שאיראן דיווחה על מתקפת סייבר נגד אחד ממפעלי הפלדה הגדולים ביותר שלה, ואף שלטענתה הצליחה לסכל את המתקפה – היא מסרה כי הייצור בו הופסק. מדובר ככל הנראה באחת מהמתקפות הגדולות ביותר נגד תעשיית הפלדה האסטרטגית של איראן, מקור ייצוא חיוני עבור כלכלתה של הרפובליקה האיסלאמית.

שר הבטחון במהדורה המרכזית

ראש הממשלה בנט במהדורה המרכזית

גנץ לחמאס אחרי פרסום תיעוד השבוי: "ניסיונות סחטנות ותרגילי תודעה לא ישפיעו על התנהלותנו"

שר הביטחון במסר תקיף לארגון הטרור בכנס הסייבר באוניברסיטת ת"א: "נמשיך להפוך כל אבן על מנת להשיב את הבנים הביתה" • הוא חשף פעילות סייבר של איראן וחיזבאללה במטרה לפגוע בפעילות כוחות יוניפי"ל בלבנון: "טרוריסטים עם מקלדת" • "איראן מובילה את טרור הסייבר – ועושה מהלכים שמטרתם להשפיע על ממשלים בעולם", הוסיף גנץ

ניר דבורי

שר הביטחון בני גנץ שלח הבוקר (רביעי) מסר תקיף לחמאס אחרי פרסום תיעוד השבוי. "ניסיונות סחטנות ותרגילי תודעה לא ישפיעו על התנהלותנו", אמר גנץ בכנס הסייבר הבין-לאומי שנערך במהלך השבוע באוניברסיטת תל אביב. שר הביטחון חשף גם פעילות סייבר של איראן וחיזבאללה נגד פעילות כוחות יוניפי"ל בלבנון: "איראן מובילה את טרור הסייבר".

"אתמול פורסם סרטון שמטרתו סחטנות על גבה של סוגיה הומניטרית, חמאס מחזיק בשבי במשך שנים את ארבעת הבנים בניגוד לחוק הבין-לאומי, בניגוד למוסר", אמר גנץ בפתח דבריו. "חמאס אחראי לכך והציפייה שלנו מהקהילה הבין-לאומית היא לפעול מול ההתנהלות הנפשעת הזו של חמאס".

שר הביטחון הבהיר כי "מדינת ישראל פועלת במגוון אמצעים, וממשיכה להפוך כל אבן על מנת להשיב את הבנים הביתה. כפי שאמרנו בעבר, מדובר בסוגיה הומניטרית, כך אנחנו רואים אותה ועל הבסיס הזה נמשיך לפעול". הוא הבהיר כי "ניסיונות סחטנות ותרגילי תודעה לא ישפיעו על התנהלותנו".

בהמשך דבריו, דיבר שר הביטחון על הפעילות הרבה של איראן בתחום הסייבר, וחשף פעילות המכוונת נגד כוחות האו"ם באזור. "איראן מפעילה את שלוחיה גם במימד הסייבר: לאחרונה אותרה פעילות של גופי הביטחון האיראניים

ראש מערך הסייבר במהדורה המרכזית

בשיתוף עם חיזבאללה, בכדי לפגוע בפעילות כוחות יוניפי"ל בלבנון". גנץ הבהיר כי מטרת האיראנים וחיזבאללה הייתה לגנוב חומרים על היערכות יוניפ"ל במרחב, לצורך שימוש של ארגון הטרור. "זוהי פגיעה נוספת של איראן וחיזבאללה באזרחי לבנון וביציבותה של לבנון", ציין גנץ.

"ישראל מכירה את מערכות הסייבר של יריביה ואת דרכי הפעולה שלהם", המשיך שר הביטחון בדבריו. "אנו רואים בשנים האחרונות תופעה של קבוצות האקרים מטעם איראן, שפועלות מול ישראל ומדינות נוספות. <השלוחים החדשים> הם טרוריסטים עם מקלדת, שדינם כמו לוחמי ארגוני טרור אחרים", הבהיר. "אנחנו יודעים מי הם, אנחנו פוגעים בהם ובשולחיהם וגם היום הם על הכוונת שלנו – ולא רק במימד הקיברנטי".

גנץ ציין כי "איראן מובילה את טרור הסייבר ועושה מהלכים שמטרתם להשפיע על תהליכים דמוקרטיים ועל ממשלים, כפי שקרה בבחירות לנשיאות ארה"ב ובניסיונות נוספים שישראל מודעת אליהם". הוא הוסיף כי "בשנים האחרונות בלמנו ניסיונות רבים לפרוץ לחברות פרטיות וציבוריות, בארץ ובחו"ל".

מוקדם יותר, השתתף בכנס מבקר המדינה מתניהו אנגלמן, שמתח ביקורת קשה בנוגע למוכנות הגנת הסייבר, גם בקרב גופים ציבוריים חשובים בישראל כמו בתי חולים, מערכות רשות המסים ועוד. "אני חייב לחלוק איתכם אמירה פסימית: אנחנו חשופים", אמר מבקר המדינה.

"לאזרחי העולם אין הגנה. הנתונים שלנו גלויים ליותר מדי אנשים. הכסף שלנו חשוף, הילדים שלנו חשופים, הבריאות שלנו חשופה, הביטחון שלנו חשוף", הבהיר אנגלמן. "מלחמת העולם השלישית תהיה מלחמת סייבר, אבל העולם לא מוכן אליה".

כלכליסט

גנץ: "בשנים האחרונות בלמנו ניסיונות רבים לפרוץ לחברות פרטיות וציבוריות"

שר הביטחון אמר את הדברים בכנס שנערך במהלך שבוע הסייבר של אוניברסיטת תל אביב. "אף מתקפה על אזרחי ישראל לא תעבור לסדר היום - והאחריות היא של התוקפים ושל המדינה שממממנת ושולחת אותם", הוסיף

רפאל קאהאן

שר הביטחון בני גנץ נאם היום (ד') במסגרת שבוע הסייבר של אוניברסיטת תל אביב וחשף מעט מקרבות הסייבר שנערכים מאחורי הקלעים בין איראן ושלוחותיה לבין ישראל ובעלות בריתה. בין השאר חשף שר הביטחון כי "לאחרונה אותרה פעילות של גופי הביטחון האיראנים בשיתוף עם חיזבאללה שמטרתה לפגוע בפעילות כוחות יוניפי"ל בלבנון על ידי מבצע סייבר לגניבת חומרים על היערכותם במרחב ושימוש בהם על ידי חיזבאללה".

גנץ תיאר את המציאות החדשה, במסגרתה איראן משתמשת בסייבר כנשק טרור המופנה לכיוון המשק הישראלי. דוגמה אחרונה לתופעה היתה בתחילת השבוע, אז נחשפו מספר מאגרי מידע של חברות תיירות שנפגעו מקבוצת האקרים בשם Sharp Boys המזוהים עם איראן.

גנץ הסביר ש"ישראל מכירה את מערכות הסייבר של יריביה ואת דרכי הפעולה שלהן. "אנו רואים בשנים האחרונות תופעה של קבוצות האקרים מטעם איראן, שפועלות מול ישראל ומדינות נוספות", אמר. "השלוחים החדשים הם טרוריסטים עם מקלדת שדינם כמו לוחמי ארגוני טרור אחרים. אנחנו יודעים מי הם, אנחנו פוגעים בהם ובשולחיהם, וגם היום הם על הכוונת שלנו. אף מתקפה על אזרחי ישראל לא תעבור לסדר היום - והאחריות היא של התוקפים ושל המדינה שממממנת ושולחת אותם. תקיפת סייבר יכולה להיענות במגוון דרכים במרחב הסייבר ובמרחבים נוספים".

שר הביטחון האשים את איראן בהעברת מבצעי הטרור שהיא מובילה למימד הסייבר. "איראן עושה מהלכים שמטרתם להשפיע על תהליכים דמוקרטיים ועל ממשלים, כפי שקרה בבחירות לנשיאות ארצות הברית ובניסיונות נוספים שישראל מודעת אליהם. פעולות כמו זו של יחידת "שאהיד כאווה" שאספה מידע על ספינות, תחנות דלק ומפעלי תעשייה במספר מדינות, נעשו תחת דירקטיבה ישירה של ההנהגה האיראנית ומשמרות המהפכה כפי שנחשף בתחקירים".

גנץ התייחס גם לחוסר המוכנות של גופים רבים במשק מבחינת הגנת סייבר. "בשנים האחרונות בלמנו ניסיונות רבים לפרוץ לחברות פרטיות וציבוריות, בארץ ובחו"ל. אני קורא גם לציבור לדרוש אחריות קיברנטית להעניש חברות וגופים שלא פועלים בהתאם להנחיות".

מנגד, חשף שר הביטחון את המאבק של כוחות הביטחון בשמירה על אנשי סייבר שהוכשרו במסגרת השירות הצבאי שלהם והודה בעקיפין שהמצב מהווה בעיה לצבא. המשכורות הגבוהות והאופק התעסוקתי המבוקש הפכו את עובדי הסייבר המנוסים של המדינה למבוקשים מאוד בקרב חברות הסייבר האזרחיות. "המשימה העליונה שלנו, בצבא, בתעשיות ובארגוני הביטחון השונים היא לבנות את האנשים, להכשיר אותם, ולהשאיר אותם", אמר גנץ.

"הרמטכ"ל ואני הצבנו את הנושא הזה כאחת המשימות המרכזיות ביחידות הרלוונטיות. אנחנו בוחנים את בניין הכוח כל העת – גם בהיקפי כוח האדם, גם בנושא ההכשרות וגם בנושא המשימות. בשנים הקרובות נצטרך גם לבחון את צורת ההתארגנות, הניהול והתפעול של לוחמת הסייבר, על מאפייניה ההתקפיים וההגנתיים בצה"ל ובמערכת הביטחון כולה".

הארץ

גנץ: איראן ערכה מתקפת סייבר נגד יוניפי"ל למען חיזבאללה

עמוס הראל ויניב קובוביץ

שר הביטחון בני גנץ אמר אתמול כי גופי הביטחון באיראן ערכו מתקפות סייבר שנועד לפגוע בכוחות יוניפי"ל בלבנון. בנאום בכנס הסייבר באוניברסיטת תל אביב אמר גנץ כי המבצע, שתוכנן בשיתוף חיזבאללה, נועד לגנוב חומרים על היערכות יוניפי"ל כדי שישמשו את חיזבאללה. "זוהי פגיעה נוספת של איראן וחיזבאללה באזרחי לבנון, וביציבותה של לבנון", אמר גנץ.

לדברי שר הביטחון, התקיפות נועדו לגנוב חומרים בעניין היערכות יוניפי"ל בלבנון

"השלוחים החדשים' הם טרוריסטים עם מקלדת שדינם כמו לוחמי ארגוני טרור אחרים", אמר גנץ. "אנחנו יודעים מי הם, אנחנו פוגעים בהם ובשולחיהם, וגם היום הם על הכוונת שלנו — ולא רק במימד הקיברנטי. שום מתקפה מול אזרחי ישראל לא תעבור לסדר היום. תקיפת סייבר יכולה להיענות במגוון דרכים במרחב הסייבר ובמרחבים נוספים".

"איראן מובילה את טרור הסייבר ועושה מהלכים שמטרתם להשפיע על תהליכים דמוקרטיים ועל ממשלים, כפי שקרה בבחירות לנשיאות ארצות הברית ובניסיונות נוספים שיראל מודעת אליהם", הוסיף גנץ. "פעולות כמו זו של יחידת 'שאהיד כאווה', שאספה מידע על ספינות, תחנות דלק ומפעלי תעשייה במספר מדינות, נעשו תחת הכוונה ישירה של ההנהגה האיראנית ומשמרות המהפכה כפי שנחשף בתחקירים".

סגן מפקד יחידת 8200 אמר בכנס כי הצבא סיכל בשנים האחרונות ניסיונות להשתלט על מערכות המים של ישראל ולהרעיל אותן, והשתלט על תוקפים שניסו לפגוע בתחנות כוח בארה"ב. "את האיום הזה הצלחנו למנוע באמצעות שיתוף פעולה הדוק עם השותפים האמריקאים שלנו", אמר בנאומו.

ישראל היום
הכי ישראלי כל הזמן

רה"מ בכנס הסייבר: "אם איראן תתעסק עם ישראל – נתקוף בכל הממדים"

"אם בעבר נדרשו 50–100 לוחמים מאחורי קווי האויב תוך סיכון עצום כדי לפגוע באויב, היום חבורה של אנשים חכמים שיושבים ליד מקלדת יכולה להשיג את אותו הדבר באמצעות סייבר" – כך אמר אתמול ראש הממשלה היוצא, נפתלי בנט, בכנס לכבוד שבוע הסייבר שנערך באוניברסיטת ת"א.

לדברי רה"מ, "באופן בלתי נמנע, הסייבר הולך להפוך לאחד המרחבים הבולטים ביותר של הלוחמה העתידית. הסייבר הוא חזית הלוחמה המודרנית. כמו שיש תרתעה גרעינית, תהיה גם תרתעה בסייבר. קצת הפתעתי מהמחסור בכלי סייבר במלחמה באוקראינה, חשבתי שזה יהיה הרבה יותר מתקדם והרבה יותר מאסיבי".

בהתייחסותו להתקדמות של ישראל בתחום הסייבר ולאיומים שהמדינה מתמודדת איתם, אמר בנט כי אם ישראל תאותגר ביכולת היא תתקוף ישירות את איראן – ולא רק בסייבר: "הגישה שלי לאויבינו, במיוחד לאיראן, היא שלא נמים הרס, אבל אם תתעסקו עם ישראל – תשלמו מחיר. אם הברירן שולח אנשים להכות אותנו, אנחנו הולכים להכות את הברירן בכל הממדים. אם מישהו יתקוף אותנו בסייבר, אנחנו נתקוף בחזרה".

רה"מ ריבר גם על אחריותם של תאגידי הענק בהתמודדות עם מתקפות זדות שמסכנות את לקוחותיהם. "תאגידים צריכים לקבל אחריות, וכשהם מתעסקים בנתוני הלקוחות שלהם זו הבעיה שלהם, אבל זה לא מספיק. ברמה הלאומית, מערך הסייבר הלאומי עובד עם החברות כדי לעזור להן להגן על עצמן, עם התשתית הקריטיות".

באשר לאקוסיסטם של הסייבר בארץ, אמר בנט: "אני רואה ארבע קבוצות שונות של כישרונות חדשים בתחום ההייטק והסייבר, שאותן אנחנו צריכים להביא כיצד משלבים – חרדים, נשים ערביות, אנשים מהפריפריה ואף פלשתינים. נתתי אישור להצטרפות מיידית של עובדים פלשתינים להייטק הישראלי, כולל אישורי תגובה לבוא לכאן".

תמיר מורג וארי אל כהנא

צילום: AP Photo/Sebastian Scheiner

"תשלמו מחיר". רה"מ בנט

ישראל היום
הכי ישראלי כל הזמן

10 א' בתמוז תשפ"ב | חמישי | 6.22

המבקר: "תהיה מלחמת עולם בסייבר, וישראל לא ערוכה"

מבקר המדינה מתניהו אנגלמן השתתף אתמול בכנס הסייבר השנתי של אוניברסיטת תל אביב, והביע חשש מפני מתקפות סייבר על ישראל. "במובן מסוים, כולנו חיים בתוך תוכנית 'האח הגדול' בינלאומית, ואני חייב לחלוק איתכם אמירה פסימית: אנחנו חשופים".

אנגלמן נתן סקירה מקיפה על ביקורת הסייבר שאותה הוא מבצע החל מכניסתו לתפקיד – או הקים אגף סייבר מיוחד.

"לאורחי העולם אין הגנה. הנתונים שלנו גלויים ליותר מדי אנשים. הכסף שלנו חשוף, הילדים שלנו חשופים, הבריאות שלנו חשופה, הביטחון שלנו חשוף. לנוכח איומי הסייבר הוולכים וגדלים שאיתם מתמודדת מדינת ישראל בשנים האחרונות, הוחלטתי להציב את תחום הסייבר כאחת מבעיות הליבה שבהן תעסוק הביקורת. הוקמו חטיבת ביקורת סייבר וחטיבה ייעודית לביקורת מערכות מידע. בהתחלה היו כאלה שלמדימו גבה". היום אין מי שלא מבין את חשיבות הנושא".

צילום: אהרן בן חקון

"נמצאו ליקויים משמעותיים"

אנגלמן סיפר כי במסגרת ביקורת הסייבר הוא בודק את הגנת הפרטיות, מנגנוני בקרה והגנה של המערכות הממוחשבות: השקעה ב־IT, הערכות מוסדי מת לאירועי סייבר והתאוששות מאסון התקפות סייבר ופגיעה בתשתיות מדינה קריטיות ועוד. כמו כן, הוא הנחה לקיים מבחני תגירה על ידי חברות האקרים מטעם משרד מבקר המדינה.

אנגלמן הוהיר כי במסגרת ביקורות הסייבר נמצאו ליקויים משמעותיים: "בשנה האחרונה ביצענו בדיקות תגירה במרכז ניהול התנועה בירושלים, בבתי חולים ובמשרכות רשות המסים. מצאנו ליקויים משמעותיים, לרבות העובדה שמעט מאוד בדיקות תגירה בוצעו על ידי גופים ציבוריים, חלקם ערכו בדיקות תגירה רק במהלך הביקורת. כמו כן, עלו ליקויים במוכנות ועדת הבחירות המרכזית לאיומי הסייבר. אנו במשרד מבקר המדינה מתחייבים להמשיך להתייחס לנושא משמעותי זה ביתר שאת, לטובת אזרחי ישראל והעולם כולו", סיכם.

יאיר אלטמן

הארץ

גנץ: איראן וחיזבאללה ביצעו התקפות סייבר כדי לפגוע בפעילות כוחות יוניפי"ל בלבנון

עמוס הראל, יניב קובוביץ

שר הביטחון בני גנץ אמר היום (רביעי) כי גופי הביטחון באיראן ערכו מתקפות סייבר שנועד לפגוע בכוחות יוניפי"ל בלבנון. בנאום בכנס הסייבר באוניברסיטת תל אביב אמר גנץ כי המבצע, שתוכנן בשיתוף חיזבאללה, נועד לגנוב חומרים על היערכות יוניפ"ל כדי שישמשו את חיזבאללה. "זוהי פגיעה נוספת של איראן וחיזבאללה באזרחי לבנון, וביציבותה של לבנון", אמר גנץ.

"<השלוחים החדשים> הם טרוריסטים עם מקלדת שדינם כמו לוחמי ארגוני טרור אחרים", אמר גנץ. "אנחנו יודעים מי הם, אנחנו פוגעים בהם ובשולחיהם, וגם היום הם על הכוונת שלנו – ולא רק במימד הקיברנטי. שום מתקפה מול אזרחי ישראל לא תעבור לסדר היום. תקיפת סייבר יכולה להיענות במגוון דרכים במרחב הסייבר ובמרחבים נוספים".

"איראן מובילה את טרור הסייבר ועושה מהלכים שמטרתם להשפיע על תהליכים דמוקרטיים ועל ממשלים, כפי שקרה בבחירות לנשיאות ארצות הברית ובניסיונות נוספים שישראל מודעת אליהם", הוסיף גנץ. "פעולות כמו זו של יחידת <שאהיד כאווה> שאספה מידע על ספינות, תחנות דלק ומפעלי תעשייה במספר מדינות, נעשו תחת הכוונה ישירה של ההנהגה האיראנית ומשמרות המהפכה כפי שנחשף בתחקירים".

סגן מפקד יחידת 8200 אמר בכנס כי הצבא סיכל בשנים האחרונות ניסיונות להשתלט על מערכות המים של ישראל ולהרעיל אותן, והשתלט על תוקפים שניסו לפגוע בתחנות כוח בארה"ב. "את האיום הזה הצלחנו למנוע באמצעות שיתוף פעולה הדוק עם השותפים האמריקאים שלנו", אמר בנאומו.

שלשום אמר ראש מערך הסייבר הלאומי, גבי פורטנוי, כי "איראן הפכה לשחקן מרכזי שאנחנו מזהים במרחב הסייבר, יחד עם חמאס וחיזבאללה". לדבריו, מערך הסייבר בלם בשנה האחרונה כ-1,500 ניסיונות תקיפה. "מגוון התוקפים בזירת הסייבר הורחב וכולל גם תוקפים נוספים – קבוצות תקיפה, שלוחות של מדינות, ארגוני פשיעה, אנשים פרטיים ועוד", אמר. פורטנוי הוסיף כי נדרשת "כיפת ברזל הגנתית בסייבר, שתגן על אזרחי ישראל ותצמצם את מתקפות הסייבר בצורה משמעותית".

ישראל היום
הכי ישראלי כל הזמן

גנץ חשף: "איראן וחיזבאללה פעלו יחד כדי לפגוע בפעילות יוניפ"ל בלבנון"

שר הביטחון השתתף בכנס הסייבר הבינלאומי באוניברסיטת תל אביב וטען כי "ישראל מכירה את מערכות הסייבר של יריביה ואת דרכי הפעולה שלהם • גנץ התייחס בין היתר לתיעוד של אל-סייד בשבי החמאס: "סרטון שמטרתו סחטנות – על גבה של סוגייה הומניטארית" • סגן מפקד יחידת 8200 חשף: "סיכלנו את הניסיון להרעיל את מערכות המים"

לילך שובל

שר הביטחון, בני גנץ נאם הבוקר (רביעי) בכנס הסייבר הבינלאומי של מרכז הסייבר באוניברסיטת ת"א ושם חשף מתקפה משותפת של איראן וחיזבאללה בכדי לפגוע בכוחות יוניפ"יל בלבנון, "פגיעה נוספת של איראן וחיזבאללה באזרחי לבנון ויציבות המדינה", אמר גנץ.

גנץ התייחס בין היתר לתיעוד של הישאם אל-סייד, השבוי בשבי החמאס בעזה, אותו שיחררה הזרוע הצבאית של ארגון הטרור: "אתמול פורסם סרטון שמטרתו סחטנות – על גבה של סוגייה הומניטארית. חמאס מחזיק בשבי את ארבעת הבנים בניגוד לחוק הבינלאומי, בניגוד למוסר. חמאס אחראית לכך והציפייה שלנו מהקהילה הבינלאומית היא לפעול מול ההתנהלות הנפשעת הזו של חמאס".

עוד הוסיף כי "מדינת ישראל פועלת במגוון אמצעים, וממשיכה להפוך כל אבן על מנת להשיב את הבנים הביתה. כפי שאמרנו בעבר – מדובר בסוגיה הומניטארית, כך אנו רואים אותה, ועל הבסיס הזה נמשיך לפעול. ניסיונות סחטנות ותרגילי תודעה לא ישפיעו על עמדתנו והתנהלותנו".

בהמשך חשף פעילות משותפת של איראן וחיזבאללה: "איראן מפעילה את שלוחיה גם במימד הסייבר: אני יכול לחשוף היום, שלאחרונה אותרה פעילות של גופי הביטחון האיראנים בשיתוף עם חיזבאללה, בכדי לפגוע בפעילות כוחות יוניפי"ל בלבנון. זאת על ידי מימוש מבצע בסייבר שמטרתו הייתה לגנוב חומרים על היערכות יוניפ"ל במרחב, ושימוש בהם על ידי חיזבאללה. זוהי פגיעה נוספת של איראן וחיזבאללה באזרחי לבנון, וביציבותה של לבנון".

"ישראל מכירה את מערכות הסייבר של יריביה ואת דרכי הפעולה שלהם. אנו רואים בשנים האחרונות תופעה של קבוצות האקרים מטעם איראן, שפועלות מול ישראל ומדינות נוספות", המשיך גנץ וסיפר. "<השלוחים החדשים>, הם טרוריסטים עם מקלדת שדינם כמו לוחמי ארגוני טרור אחרים. אנחנו יודעים מי הם, אנחנו פוגעים בהם ובשולחיהם, וגם היום הם על הכוונת שלנו – ולא רק במימד הקיברנטי. שום מתקפה מול אזרחי ישראל לא תעבור לסדר היום. והאחריות היא של התוקפים ושל המדינה שממממנת ושולחת אותם. תקיפת סייבר יכולה להיענות במגוון דרכים במרחב הסייבר ובמרחבים נוספים".

גנץ המשיך במתקפה על מעצמת הגרעין: "איראן מובילה את טרור הסייבר – ועושה מהלכים שמטרתם להשפיע על תהליכים דמוקרטיים ועל ממשלים, כפי שקרה בבחירות לנשיאות ארצות הברית ובניסיונות נוספים שישראל מודעת אליהם. פעולות כמו זו של יחידת <שאהיד כאווה> שאספה מידע על ספינות, תחנות דלק ומפעלי תעשייה במספר מדינות, נעשו תחת דירקטיבה ישירה של ההנהגה האיראנית ומשמרות המהפכה כפי שנחשף בתחקירים".

עוד הוסיף כי "בשנים האחרונות בלמנו ניסיונות רבים לפרוץ לחברות פרטיות וציבוריות, בארץ ובחו"ל. אני קורא גם לציבור לדרוש <אחריות קיברנטית>, ולהעניש חברות וגופים שלא פועלים בהתאם להנחיות".

גנץ המשיך וסימן את היעדים הבאים של ישראל מול האיומים: "המשימה העליונה שלנו, בצבא, בתעשיות ובארגוני הביטחון השונים היא לבנות את האנשים, להכשיר אותם, ולהשאיר אותם. אני והרמטכ"ל הצבנו את הנושא הזה כאחת המשימות המרכזיות ביחידות הרלבנטיות. אנחנו בוחנים את בניין הכוח כל העת – גם בהיקפי כוח האדם, גם בנושא ההכשרות וגם בנושא המשימות. בשנים הקרובות נצטרך גם לבחון את צורת ההתארגנות, הניהול והתפעול של לוחמת הסייבר, על מאפייניה ההתקפיים וההגנתיים בצה"ל ובמערכת הביטחון כולה".

לבסוף סיכם שר הביטחון וקרא לשיתופי פעולה עם העולם: "יש חשיבות גדולה לשיתופי הפעולה שלנו עם העולם מול איראן גם במימד הסייבר. את אותם שיתופי פעולה שאנו בונים באזור מול איראן בהיבטים של הגנה מול איומים שונים – אנחנו מרחיבים גם במימד הסייבר".

סגן מפקד יחידת 8200 חשף: "סיכלנו את הניסיון להרעיל את מערכות המים"

אורי, סגן מפקד יחידת 8200, אמר בהופעה הפומבית הראשונה של היחידה בכנסים מסוג זה, חשף כי ישראל סיכלה התקפה על מערכות המים.

"סיכול איומי סייבר הוא חלק מרכזי בפעילות שלנו. מטרתנו להשיג עליונות על התוקף, להצליח לזהות אותו ולפעול כדי לשלול את יכולותיו". אמר סגן מפקד 8200 והוסיף "כך לעיתים אנו גם מוצאים קורבנות מחוץ לישראל ואז אנו יוצרים קשר עם סוכניות אחרות אם צריך. אנו עושים זאת גם באופן עצמאי וגם על ידי שיתוף פעולה עם התעשייה וסוכנויות אחרות, באמצעות יישום ושימוש בכלים שפיתחנו. 8200 לא תנוח עד שהאיום יוסר".

כאמור, כך נחשף איום על מערכות המים של ישראל והניסיונות להרעיל את אזרחי ישראל: "סיכלנו את הניסיון להשתלט על מערכות המים הקריטיות של ישראל ולהרעיל אותן לפני מספר שנים. במקרה אחר זיהינו גם כי יריב מסוים תקף את ישראל ותוך כדי זיהינו שאותו תוקף ניסה גם לכוון לתחנות כוח בארה"ב. זו הייתה האינדיקציה הראשונה להתקפה זו. את האיום הזה הצלחנו למנוע באמצעות שיתוף פעולה הדוק עם השותפים האמריקאים שלנו".

ynet
ידיעות אחרונות

מבקר המדינה: "מלחמת העולם השלישית תהיה מלחמת סייבר והעולם לא מוכן"

מבקר המדינה סיפק במסגרת שבוע הסייבר השנתי של אוניברסיטת תל אביב סקירה מקיפה וראשונה על מצב הסייבר בעולם ובישראל: "אנחנו חשופים ונטולי הגנה. כולנו חיים בתוך תוכנית עולמית של האח הגדול. מצאנו ליקויים רבים"

רועי האן

מבקר המדינה מתניהו אנגלמן השתתף הבוקר (ד<) בשבוע הסייבר השנתי של אוניברסיטת תל אביב, וסיפק סקירה מקיפה ראשונה אודות מצב הסייבר בארץ ובעולם. דבריו על תמונת המצב בישראל עלו מביקורת הסייבר, שהחל לבצע במסגרת אגף הסייבר שהקים עם כניסתו לתפקיד.

"הסייבר היום חשוב מתמיד", פתח אנגלמן. "במבן מסוים, כולנו חיים בתוך תוכנית עולמית של האח הגדול. אני חייב לחלוק איתכם אמירה פסימית: אנחנו חשופים. לאזרחי העולם אין הגנה. הנתונים שלנו גלויים ליותר מידי אנשים. הכסף שלנו חשוף, הילדים שלנו חשופים, הבריאות שלנו חשופה, הביטחון שלנו חשוף. מלחמת העולם השלישית תהיה מלחמת סייבר שהעולם לא מוכן אליה".

מטרת אגף הסייבר שהקים אנגלמן היא לבחון את העמידות והחוסן של ישראל בהתמודדות עם אירועי סייבר. לדבריו, בשנה האחרון ביצע האגף מספר בדיקות עמידות וחדירה במספר ארגונים בתעשייה הישראלית, בהם המרכז לניהול התנועה בירושלים, בתי חולים בכל הארץ והמערכות של רשות המיסים. "מצאנו ליקויים משמעותיים בביקורות שערכנו, לרבות העובדה שמעט מאוד בדיקות חדירה בוצעו על ידי הגופים הציבוריים - חלקם אף ערכו בדיקות רק במהלך הביקורת שלנו", אמר אנגלמן. "משרד מבקר המדינה מתחייב להמשיך ולהתייחס לנושא המשמעותי הזה ביתר שאת, לטובת אזרחי ישראל והעולם כולו".

אנגלמן סיפר כי במסגרת הביקורות שערך המשרד נבדקות גם מערכות הגנת הפרטיות וכן מנגנוני הבקרה וההגנה של המערכות הממוחשבות. בנוסף נבדקת גם ההשקעה ב-IT, היכולת להיערכות מוקדמת לאירועי סייבר, יכולות ההתאוששות מאסון, עמידות בהתקפות סייבר ופגיעה בתשתיות מדינה קריטיות.

אנגלמן התייחס גם לעמידות של ועדת הבחירות המרכזית בישראל לקראת הבחירות הקרובות: "דו"ח הבדיקה שלנו על הוועדה מצא כי מערכת המחשוב המרכזית שלה החלה לפעול בשנת 2008 - היא חגגה בת מצווה בשנה שעברה. ועדיין, ביקורות הסייבר נערכו רק בתקופות בחירות, כך שלא ניתן היה לבצע בדיקות מקיפות ומורכבות שכללו את כל ההיבטים החדשים להגנת הסייבר של ימינו".

מעריב

מבקר המדינה מזהיר: "ועדת הבחירות המרכזית לא ערוכה לאיומי סייבר"

מבקר המדינה מתניהו אנגלמן השתתף בכנס הסייבר של אוניברסיטת תל אביב, סקר את מוכנותה של ישראל להגנה על אזרחיה מפני מתקפות סייבר והזהיר: "מלחמת העולם השלישית תהיה מלחמת סייבר - אך העולם לא ערוך אליה"

אריק בנדר

מבקר המדינה מתניהו אנגלמן השתתף היום (רביעי) בשבוע הסייבר השנתי בהובלת המרכז למחקר סייבר באוניברסיטת ת"א, מערך הסייבר הלאומי, משרד הכלכלה ומשרד החוץ, וסקר לראשונה באופן מקיף את ביקורת הסייבר אותה הוא מבצע החל מכניסתו לתפקיד. הוא סיפר כי במסגרת הבדיקות "עלו ליקויים משמעותיים במוכנות ועדת הבחירות המרכזית לאיומי הסייבר" והזהיר: "מלחמת העולם השלישית תהיה מלחמת סייבר - אך העולם לא ערוך אליה".

"הסייבר היום חשוב מתמיד", פתח אנגלמן. "במובן מסוים, כולנו חיים בתוך תכנית <האח הגדול> בינלאומית. כמבקר מדינת ישראל וסגן נשיא EUROSAI, אני חייב לחלוק איתכם אמירה פסימית: אנחנו חשופים. לאזרחי העולם אין הגנה. הנתונים שלנו גלויים ליותר מדי אנשים. הכסף שלנו חשוף, הילדים שלנו חשופים, הבריאות שלנו חשופה, הביטחון שלנו חשוף. מלחמת העולם השלישית תהיה מלחמת סייבר, אבל העולם לא מוכן אליה".

הוא המשיך ואמר: "עם כניסתי לתפקיד הנוכחי של מבקר המדינה, ולנוכח איומי הסייבר ההולכים וגדלים איתם מתמודדת מדינת ישראל בשנים האחרונות, החלטתי להציב את תחום הסייבר כאחד מבעיות הליבה בהן תעסוק הביקורת. הוקמו חטיבת ביקורת סייבר וחטיבה ייעודית לביקורת מערכות מידע. בהתחלה היו כאלה ש<הרימו גבה>. היום אין מי שלא מבין את חשיבות הנושא. גם ארגון המבקרים הבינלאומי קבע כי הגנה כזו על מערכות מידע היא אחד הסיכונים הגדולים ביותר".

אנגלמן סיפר כי במסגרת ביקורות הסייבר הוא בודק את הגנת הפרטיות, מנגנוני בקרה והגנה של המערכות הממוחשבות; השקעה ב-IT, היערכות מוקדמת לאירועי סייבר והתאוששות מאסון, התקפות סייבר ופגיעה בתשתיות מדינה קריטיות. ועוד. כמו כן, הוא הנחה לקיים מבחני חדירה על ידי חברות האקרים מטעם משרד מבקר המדינה.

אנגלמן הוסיף כי "דו"ח על מערכת המחשוב של ועדת הבחירות המרכזית בישראל מצא כי מערכת המחשוב המרכזית שלהם החלה לפעול בשנת 2008 והיא חגגה "בר מצווה" בשנה שעברה. ועדיין, ביקורות סייבר נערכו רק בתקופות בחירות, כך שלא ניתן היה לבצע בדיקות מקיפות ומורכבות שכללו את כל ההיבטים הנדרשים להגנת הסייבר".

"בשנה האחרונה ביצענו בדיקות חדירה במרכז ניהול התנועה בירושלים, בבתי חולים ובמערכות רשות המסים. בביקורות מצאנו ליקויים משמעותיים, לרבות העובדה שמעט מאוד בדיקות חדירה בוצעו על ידי גופים ציבוריים וחלקם ערכו בדיקות חדירה רק במהלך הביקורת; אנו במשרד מבקר המדינה מתחייבים להמשיך ולהתייחס לנושא משמעותי זה ביתר שאת, לטובת אזרחי ישראל והעולם כולו", סיכם המבקר.

כלכליסט

מבקר המדינה: "הילדים שלנו חשופים, הביטחון שלנו חשוף, הכסף שלנו חשוף"

המבקר מתניהו אנגלמן אמר את הדברים במהלך שבוע הסייבר של אוניברסיטת תל אביב, שם התייחס גם באופן ספציפי לאפשרות של שיבוש מערכת הבחירות המתקרבת בידי האקרים: "יש ליקויים משמעותיים במוכנות של ועדת הבחירות המרכזית לאיומי הסייבר"

רפאל קאהאן

מבקר המדינה מתניהו אנגלמן אמר היום (ד<) בשבוע הסייבר הבינלאומי של אוניברסיטת תל אביב: "עלו ליקויים משמעותיים במוכנות ועדת הבחירות המרכזית לאיומי הסייבר". אנגלמן התייחס לראשונה לאגף הסייבר שהוקם במשרדו וסקר את הביקורות שאותן החל לבצע.

"במובן מסוים, כולנו חיים בתוך תכנית <האח הגדול> בינלאומית. כמבקר מדינת ישראל, אני חייב לחלוק איתכם אמירה פסימית: אנחנו חשופים. לאזרחי העולם אין הגנה. הנתונים שלנו גלויים ליותר מדי אנשים. הכסף שלנו חשוף, הילדים שלנו חשופים, הבריאות שלנו חשופה, הביטחון שלנו חשוף. מלחמת העולם השלישית תהיה מלחמת סייבר, אבל העולם לא מוכן אליה".

וד סיפר אנגלמן כי במסגרת ביקורות הסייבר הוא בודק את הגנת הפרטיות, מנגנוני בקרה והגנה של המערכות הממוחשבות, השקעה ב-IT, היערכות מוקדמת לאירועי סייבר והתאוששות מאסון, התקפות סייבר ופגיעה בתשתיות מדינה קריטיות. ועוד. כמו כן, הוא הנחה לקיים מבחני חדירה על ידי חברות האקרים מטעם משרד מבקר המדינה.

"דו"ח על מערכת המחשוב של ועדת הבחירות המרכזית בישראל מצא כי מערכת המחשוב המרכזית שלהם החלה לפעול בשנת 2008 והיא חגגה <בר מצווה> בשנה שעברה. ועדיין, ביקורות סייבר נערכו רק בתקופות בחירות, כך שלא ניתן היה לבצע בדיקות מקיפות ומורכבות שכללו את כל ההיבטים הנדרשים להגנת הסייבר". זהו איום ממשי על טוהר הבחירות במדינה - הגם שההצבעה בפועל מתבצעת עדיין על פתקי נייר, ככל הנראה כנגזרת מאיומי הסייבר הפוטנציאליים".

בנוסף, אנגלמן אמר שהוא מודאג מאוד מהמצב בשטח והסביר שבשנה האחרונה בוצעו בדיקות חדירה במרכז ניהול התנועה בירושלים, בבתי חולים ובמערכות רשות המסים, בהן נמצאו ליקויים משמעותיים. העיקרי שבהם הוא מיעוט בדיקות החדירה שבוצעו על ידי גופים ציבוריים. בנוסף, אמר אנגלמן שחלקם ערכו בדיקות חדירה רק במהלך הביקורת. בדיקות אלה משמשות לבחינת ההיערכות של הגופים לתקיפות סייבר ונערכות על ידי חברות המתמחות בתהליך, שמדמות תקיפות האקרים על מגוון מערכות, תוך שימוש בכלי תקיפה נפוצים. התוצאה כאמור מדאיגה ומעמידה בספק את היכולת של חלק ניכר מהגופים האלה להתמודד עם מתקפות סייבר.

ישראל היום
הכי ישראלי כל הזמן

מבקר המדינה מזהיר: "ועדת הבחירות המרכזית לא ערוכה לאיומי הסייבר"

מתניהו אנגלמן התריע בשבוע הסייבר הבינלאומי מפני חוסר המוכנות של ישראל לתקיפות פצחנים • "מלחמת העולם השלישית תהיה מלחמת האקרים אך העולם לא ערוך אליה"

יאיר אלטמן

מבקר המדינה מתניהו אנגלמן השתתף היום (רביעי) בכנס הסייבר השנתי של אוניברסיטת תל אביב והביע חשש מפני מתקפות סייבר על ישראל. "אנחנו חשופים. הנתונים שלנו גלויים ליותר מדי אנשים. הכסף שלנו חשוף, הילדים שלנו חשופים, הבריאות שלנו חשופה, הביטחון שלנו חשוף. מלחמת העולם השלישית תהיה מלחמת סייבר, אבל העולם לא מוכן אליה".

אנגלמן סיפר כי במסגרת ביקורות הסייבר שמשרדו עורך, נמצאו ליקויים משמעותיים: "בשנה האחרונה ביצענו בדיקות חדירה במרכז ניהול התנועה בירושלים, בבתי חולים ובמערכות רשות המיסים. בביקורות מצאנו ליקויים משמעותיים, לרבות העובדה שמעט מאוד בדיקות חדירה בוצעו על ידי גופים ציבוריים וחלקם ערכו בדיקות חדירה רק במהלך הביקורת. בנוסף עלו ליקויים במוכנות ועדת הבחירות המרכזית לאיומי הסייבר".

"אנו במשרד מבקר המדינה מתחייבים להמשיך ולהתייחס לנושא משמעותי זה ביתר שאת, לטובת אזרחי ישראל והעולם כולו", סיכם.

ISRAELDEFENSE

מנכ"ל ומייסד סייבראר‍ק: לעובד ממוצע יש כיום יותר מ-30 זהויות דיגיטליות

"הזהויות מפוזרות כיום בכל מקום. בענן, על תחנות קצה, בתהליכי הפיתוח ולרוחב שרשרת האספקה", הסביר אודי מוקדי, מנכ"ל ומייסד סייבראר‍ק

עמי רוחקס דומבה

"הזהויות הדיגיטליות, שמספרן מגיע למאות ואלפי זהויות לארגון, יוצרות חוב אבטחה שהולך ומצטבר, מה שחושף ארגונים לסיכונים מוגברים, כגון: דליפת סיסמאות, שימוש זדוני בזהות ארגונית לבצע גישה לא מורשית למידע ועוד", אמר אודי מוקדי, מנכ"ל ומייסד סייבראר‍ק הציג בכנס שבוע הסייבר באוניברסיטת ת"א.

לפי סקר שערכה החברה, לעובד ממוצע יש כיום יותר מ-30 זהויות דיגיטליות. יותר מכך, מספר זהויות המכונה עולה כיום על מספר הזהויות האנושיות פי 45 בממוצע.

לדברי מוקדי, "כל יוזמת מחשוב או דיגיטציה ארגונית מרכזית מובילה לגידול במספר האינטראקציות בין בני אדם, יישומים ותהליכים, מה שמוביל להיווצרותן של זהויות דיגיטליות רבות – של בני אנוש ושל מכונות. השימוש בזהויות דיגיטליות אלו מקל על האינטראקציות ועל הגישה של גורמי צד שלישי למידע ארגוני רגיש ולנכסי מידע הנדרשים כדי לבצע עבודה או פונקציה כלשהי.

"הזהויות מפוזרות כיום בכל מקום. בענן, על תחנות קצה, בתהליכי הפיתוח ולרוחב שרשרת האספקה. זו הסיבה שאנחנו קוראים לזהות שדה הקרב הבא של אבטחת הסייבר".

סייבראר‍ק מצאה גם, של-52% מכוח האדם בארגונים שנסקרו יש גישה כלשהי למידע רגיש, בעוד של-68 אחוזים מהזהויות הלא-אנושיות או מהבוטים יש גישה לנתונים ונכסי מידע רגישים.

"פלטפורמת אבטחת הזהויות של סייבראר‍ק מספקת פתרון מקיף להגנה על זהויות – אנושיות או של מכונות – באפליקציות ארגוניות, בכוח עבודה מבוזר, בעומסי עבודה היברידיים בענן ולאורך כל תהליכי הפיתוח ב- DevOps", סיכם מוקדי.

Forbes Israel

סגן מפקד 8200 חושף את הנשק הסודי של יחידת המודיעין המובחרת

הבכיר גילה כי סוכלו ניסיונות להרעיל את מי השתייה בישראל. "רב החיילים ביחידה שלנו הם מתחת לגיל 23 וזה סוד הקסם של היחידה"

"סיכלנו את הניסיון להשתלט על מערכות המים הקריטיות של ישראל ולהרעיל אותן." כך סיפר היום בכיר ביחידת 8200 בשבוע הסייבר השנתי בסימן "הנוף העתידי של עולם אבטחת הסייבר" באוניברסיטת תל אביב. במסגרת האירוע, המתקיים זו השנה ה-12, מרצים מיטב המומחים ובכירי התעשייה העולמית, בנוסף לכנסים וסדנאות שונות.

השנה מובילים את הפאנל: ראש ממשלת ישראל החליפי נפתלי בנט, שר הביטחון בני גנץ, ראש מערך הסייבר הלאומי גבי פורטנוי, וסגן מפקד יחידת 8200, אשר נאם בפנים גלויות ואף חשף כי היחידה סיכלה ניסיונות להשתלטות על מערכות המים הקריטיות של ישראל. "זוהי ההופעה הפומבית הרשמית הראשונה של 8200" אמר במהלך הנאום, "זאת למרות שמזה כבר כמה עשרות שנים אנחנו מהווים חלק ניכר ממערך ההגנה והמודיעין של ישראל והמשימה שלנו היא איסוף מודיעין על איומים מכריעים על ישראל".

סגן המפקד ביחידת 8200 סיפר כי מלבד סיכול הניסיון להשתלטות מקורות קריטיים בישראל, "זיהינו גם כי יריב מסוים תקף את ישראל ותוך כדי זיהינו שאותו תוקף ניסה גם לכוון לתחנות כוח בארה"ב. זו הייתה האינדיקציה הראשונה להתקפה זו. את האיום הזה הצלחנו למנוע באמצעות שיתוף פעולה הדוק עם השותפים האמריקאים שלנו. הישגים כאלו הם שגורמים לחיילים שלנו להיות גאים בעבודתם ב-8200."

הוא עוד הוסיף כי "ידוע לכל שאנחנו מהווים שחקן מרכזי בתחום הסייבר בישראל ומעבדים את המידע באמצעות כלים שפותחו אצלנו. המידע שאנו מקבלים מגיע ממקורות שונים משותפים, ובעיקר בזכות פעולה אקטיבית במרחב הסייבר אל מול רשתות יעד ותשתיות ארגוני טרור. אנחנו חיים בסביבה קשה וזה מצריך מאיתנו לעבוד קשה בסביבה דינמית ואינטנסיבית שמספקת אתגרים חדשים מדי יום. כשאנחנו מצליחים אנחנו מצילים חיים. כשאנחנו נכשלים זה הופך לבעיה גדולה עבור האומה שלנו".

ידיעות אחרונות

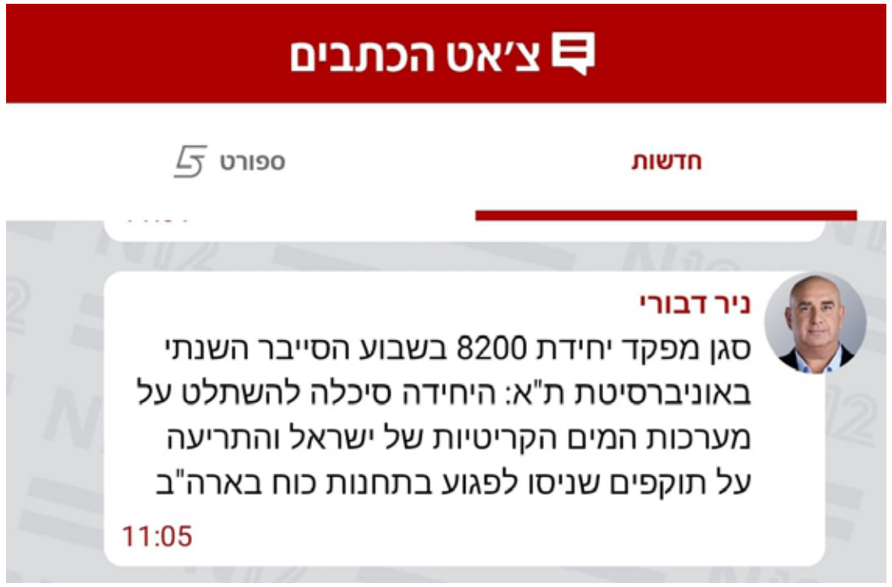
בנט: "מחקפת סייבר חיענה במחקפה"

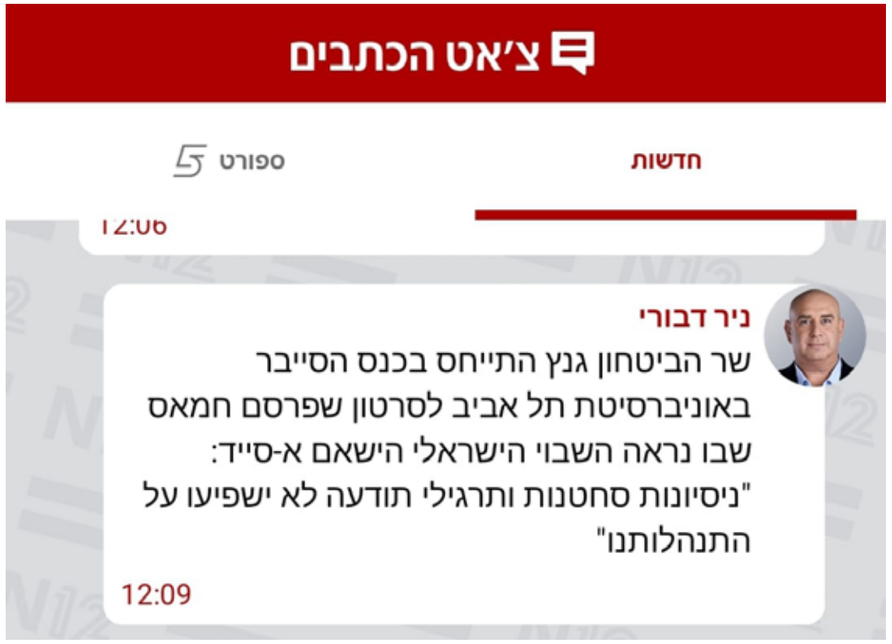
ראש הממשלה נפתלי בנט התייחס לסוגיית מתקפות הסייבר אתמול, בשבוע הסייבר השנתי באוניברסיטת תל־אביב.

בנט אמר כי "מה שדרש בעבר אנשי קומנדו שיפעלו בסודיות מאחורי קווי האויב, אפשר להשיג היום באמצעות כמה אנשים חכמים שיושבים עם מקלדת".

ראש הממשלה התייחס גם לאיום האיראני ואמר כי "אם אתה מתעסק עם ישראל – תשלם מחיר. אם מישהו תוקף אותנו באמצעות סייבר, אנחנו נתקוף חזרה".

נינה פוקס


צ'אט הכתבים
חדשות
ספורט
ניר דבורי
סגן מפקד יחידת 8200 בשבוע הסייבר השנתי באוניברסיטת ת"א: היחידה סיכלה להשתלט על מערכות המים הקריטיות של ישראל והתריעה על תוקפים שניסו לפגוע בתחנות כוח בארה"ב
11:05


צ'אט הכתבים
חדשות
ספורט
ניר דבורי
שר הביטחון גנץ התייחס בכנס הסייבר באוניברסיטת תל אביב לסרטון שפרסם חמאס שבו נראה השבוי הישראלי הישאם א-סייד: "ניסיונות סחטנות ותרגילי תודעה לא ישפיעו על התנהלותנו"
12:09

PC אנשים ומחשבים

"הצלחנו לעצור מתקפות על מתקני המים בישראל ותחנות כוח בארה"ב"

אל"מ אורי, סגן מפקד 8200, ציין שישראל עצרה את שתיהן● מבקר המדינה: "עלו ליקויים משמעותיים במוכנות ועדת הבחירות למתקפות סייבר"

יניב הלפרין

ישראל עצרה את המתקפה האיראנית על מקורות המים שלה, כמו גם מתקפה שפגעה בארצות הברית – כך אמר היום (ד>) סא"ל אורי, סגן המפקד של יחידה 8200, בשבוע הסייבר באוניברסיטת תל אביב.

לדברי סא"ל אורי, "סיכלנו לפני מספר שנים את הניסיון להשתלט על מערכות המים הקריטיות של ישראל ולהרעיל אותן. במקרה אחר זיהינו שיריב מסוים תקף את ישראל, ותוך כדי זיהינו שאותו תוקף ניסה גם לכוון לתחנות כוח בארצות הברית. את האיום הזה הצלחנו למנוע באמצעות שיתוף פעולה הדוק עם השותפים האמריקניים שלנו".

המתקפה, שדווחה בראשונה ב-ynet, אירעה ב-24 וב-25 באפריל 2020, ופגעה במתקני מים וביוב מצפון הארץ ועד לדרומה. הפיינגשל טיימס פרסם חודש לאחר מכן דיווח מפורט יותר על המתקפה, שבו ציין העיתון שהאיראנים הצליחו לפרוץ למערכות שמתפעלות את משאבות המים בישראל, תוך שימוש בשרתים הממוקמים בארצות הברית ובאירופה, וניסו להחדיר אליהן כמות רבה של כלור. אילו המתקפה הייתה מצליחה, אזרחים ישראליים רבים היו מורעלים וחולים, וייתכן שאחרים היו נותרים ללא מים. כן דווח שכנקמה על המתקפה, ישראל ביצעה מתקפת סייבר על נמל באיראן, שפגעה כלכלית ברפובליקה האסלאמית.

"העולם, כולל ישראל, לא ערוך למלחמת העולם השלישית – שתהיה בסייבר"

מבקר המדינה, מתניהו אנגלמן, חזר באירוע על אזהרותיו בדו"חות שפרסם, שלפיה ישראל לא ערוכה היטב להגנה מפני אירועי סייבר, שלא לומר מפני מלחמת עולם שלישית שלדעתו תפרוץ ותתמקד במתקפות ממוחשבות. כמו כן, הוא ציין כי "עלו ליקויים משמעותיים במוכנות ועדת הבחירות המרכזית לאיומי הסייבר". המבקר אמר שמערכות המחשוב של ועדת הבחירות נבדקות מפני אירועי סייבר רק בתקופות של מערכות בחירות, ולא באופן שוטף.

"אנחנו חשופים, נטולי הגנה, חיים בתוך תוכנית עולמית של האח הגדול. מלחמת העולם השלישית תהיה מלחמת סייבר, אך העולם לא ערוך אליה, כולל ישראל", התריע אנגלמן.

"אדם אחד שלא שמר טוב על המחשב גרם למתקפה על הביטחון של ארה"ב"

בין הדוברים באירוע היו שני בכירים בתחום הסייבר מהבית הלבן. כריס אינגליס, מנהל הסייבר הלאומי בממשל ביידן, אמר כי "יש לוודא שהסייבר מגן על הדברים שמשרתים את חיינו, כגון תשתיות ו-IT".

אינגליס התייחס למתקפה על קולוניאל פייפליין, שאירעה במאי אשתקד והביאה לשיבוש ניכר באספקת הדלק בחלק המזרחי של ארצות הברית. "בחקירת המתקפה הזו מצאנו שאדם אחד שלא שמר טוב מספיק על מערכת המחשוב שלו אפשר, למעשה, להאקרים להיכנס ולתקוף רשת גדולה באירוע שהיווה מתקפה על הביטחון הלאומי של ארצות הברית. ההאקרים למדו לקח מהאירוע הזה, ומצאו שאם הם יכולים לתקוף אחד מאתנו – הם יכולים לתקוף את כולנו". באשר למתקפה גדולה אחרת, Log4j, שפגעה בגופי ממשל ובחברות פרטיות בארצות הברית, הוא אמר כי "אילו היינו מגלים אותה מוקדם יותר, היינו מפסידים פחות".

הבכיר האמריקני קרא לשיתוף פעולה הדוק יותר בין גופים ממשלתיים והמגזר הפרטי להגנה מפני מתקפות סייבר. "הממשלה יכולה להשתמש בכלים דיפלומטיים, בכלי אכיפת חוק ובמודיעין כדי להילחם בסייבר, והמגזר הפרטי יכול להביא למשוואה את היכולות והטכנולוגיות שלו. אנחנו צריכים לדעת מה יקרה, מתי ומאיזו דלת ההאקר ייכנס. הדרך היחידה שלנו לראות את זה בזמן היא לשלב את המקורות ואת תחומי האחריות שלנו, במגזרים הממשלתי והפרטי. יש דברים שאנחנו לא יכולים לעשות לבד, אבל כן יכולים לעשות ביחד. זה גם ישדר להאקרים שכדי להכות באחד מאתנו, הם צריכים להכות בכולנו", אמר.

"שמירה על התשתיות הקריטיות מגנה על קבלת ההחלטות ברמת המדינה"

אן נויברגר, סגנית היועץ לביטחון לאומי של ארצות הברית לענייני סייבר וטכנולוגיות מתפתחות, אמרה כי "בשנה וחצי האחרונות, מאז כניסתו של ג>ו ביידן לבית הלבן, אנחנו פועלים רבות בתחום הסייבר. בתקופה הזאת היינו צריכים להגן על מערכות הבריאות, ומול היבטי הסייבר של המלחמה הפרובוקטיבית של רוסיה מול אוקראינה".

"הנשיא ביידן הגביר את הטיפול בסוגיות סייבר בארצות הברית: אבטחת סייבר ושיתופי פעולה עם בעלות הברית שלנו ברחבי העולם", אמרה. לדבריה, שיתופי הפעולה האלה "מעלים את האמון, מביאים לשיתוף ידע באשר לטכניקות של ההאקרים, שהרבה פעמים הן דומות, ושומר על הביטחון והיציבות בעולם".

גם נויברגר התייחסה למתקפה על קולוניאל פייפליין ואמרה כי "היא הראתה לנו איך מתקפת סייבר יכולה לשבש את החיים והכלכלה. למדנו בעקבותיה ששמירה על תשתיות קריטיות מגנה על קבלת ההחלטות שלנו, כמדינה".

נויברגר קראה "לעבוד ביחד כדי לפתח תוכנה וחומרה עם סייבר בילט אין; לבנות את הדורות הבאים של הגנת הרשתות, כדי לחסום פעילות עוינת בסייבר; ולהגביר את העבודה עם שותפים ברחבי העולם. אנחנו מאמינים בבניית מכניזמים לעבודה בינלאומית בסייבר ביחד, לבנות קואליציות לטיפול באיומי הסייבר, כי בסופו של דבר, כולנו באותה הסירה. אני מקווה שעוד מדינות יצטרפו להגנה קולקטיבית בתחום הסייבר".

» דיווח בכאן ב'

חמאס מוכן לאפשר כניסת ישראלי לעזה כדי לקדם עסקת חילופי שבויים

מתן וסרמן, אלון חכמון

חמאס הסכים לאפשר בניסת אזרח ישראלי לעזה בניסיון לחניע מגעים לעסקת שבויים. בישראל עודכנו בפרטים. כך דיווח אתמול בכאן ב'.

זאת ימים לאחר פרסום תיעוד השבוי הישראלי הישאם א'סייד כשהוא מחובר למכונת חמצן. לפי הדיווח, סאמי עובייד, פעיל ציבורי בעזה, ויואל מרשק, איש התנועה הקיבוצית, פועלים לקדם יוזמה אזרחית להנעת פתרון לסוגיית השבויים והנעדרים, שבמסגרתה קיבל מרשק אישור עקרוני מחמאס להיכנס לרצועה.

עוד דווח כי בחודש וחצי האחרון מרשק נפגש עם אישיות ביטחונית בכירה בישראל ועדכן אותו בנושא היוזמה וההסכמה העקרונית של חמאס. הוא ביקש לתת לו להיכנס לרצועה כדי לקדם את הנושא. אותה אישיות ביטחונית בכירה אמרה לו שהנושא ייבדק.

פרופ' שמחה גולדין, אביו של סגן הדר גולדין, שוחח אתמול עם גולן יוכפז וענת דוידוב ברדיו 103FM. בפתח דבריו אמר פרופ' גולדין: "אנחנו אומרים את זה פחות או יותר מהיום הראשון. ברור שלא יעלה על הדעת שהממשלה מקדמת הסכמול חמאס, שלא כולל את הלוחמים שנשלחו על ידי גנץ ונתניהו. אנחנו מתעסקים עם ארגון טרור. החיילים שיוצאים להגן על האזרחים צריכים להיות מושבים. אנחנו אומרים את זה שמונה שנים".

עוד אמר: "הפקדתי את הילדים שלי בידי המדינה. המפקד שלהם בזמן הלחימה היה גנץ. הוא שלח אותם להילחם נגד אויב שרצה להרוג אותנו, אותי ואתכם. הדר לא היה בעזה כדי לטייל שם, שלחו אותו להרוג את מי שרוצה להרוג אותנו. מאז לא מש[illegible] אותו [illegible] שאל האחראים [illegible]

שר הביטחון בני גנץ התייחס לנושא אתמול בנאום שנשא בשבוע הסייבר באוניברסיטת ת"ל אביב והגיב לסרטון שפרסם חמאס, שבו נראה השבוי הישראלי הישאם א'סייד כשהוא מחובר למכשיר חמצן: "מטרת הסרטון היא סחטנות על גבה של סוגייה הומניטרית. חמאס מחזיק בשבי במשך שנים את ארבעת הבנים, זאת בניגוד לחוק הבינלאומי והמוסר".

[illegible] מוחמד מאהר מרעי, בן 23, שמו[illegible] על יד[illegible] בוחות הביטחון במחבל העוסק ב[illegible] עלות טרור, נהר[illegible] במהול בבוקר מירי אל[illegible] בוחות צה"ל בג'נין. מרעי נפצע [illegible] עם שניים מחבריו על ידי כוחות שפעלו בעיר ומאוחר יותר מת מפצעיו בבית החולים. מקורות פלסטיניים מציינים כי מרעי הוא בן דודו של המחבל בראא אל-לחלול, אחד מהמחבלים שחוסלו לפני כשבועיים בג'נין.

בנוסף פעלו כוחות של מג"ב, שב"כ וצה"ל במהלך הלילה ברחבי יהודה ושומרון וביצעו מעצרים של 13 חשודים בפעולות טרור וביטחון. לא היו נפגעים לכוחותינו.

גנץ. "מטרת הסרטון היא סחטנות"
צילום: אבשלום ששוני

בכיר ב-8200 חשף כי היחידה סיכלה ניסיונות להשתלט על מערכת קריטית בישראל

אורי, סגן מפקד יחידת 8200, נשא נאום במהלך שבוע הסייבר השנתי: "כשאנחנו מצליחים אנחנו מצילים חיים. כשאנחנו נכשלים זה הופך לבעיה גדולה עבור האומה שלנו"

סתיו נמר

אורי, סגן מפקד יחידת 8200, נשא הבוקר (רביעי) נאום במהלך בשבוע הסייבר השנתי בהובלת המרכז למחקר סייבר באוניברסיטת ת"א, מערך הסייבר הלאומי, משרד הכלכלה ומשרד החוץ. בראשית דבריו, הקצין ציין כי "זוהי ההופעה הפומבית הרשמית הראשונה של 8200, זאת למרות שמזה כבר כמה עשרות שנים אנחנו מהווים חלק ניכר ממערך ההגנה והמודיעין של ישראל והמשימה שלנו היא איסוף מודיעין על איומים מכריעים על ישראל"."ידוע לכל שאנחנו מהווים שחקן מרכזי בתחום הסייבר בישראל ומעבדים את המידע באמצעות כלים שפותחו אצלנו. המידע שאנו מקבלים מגיע ממקורות שונים משותפים, ובעיקר בזכות פעולה אקטיבית במרחב הסייבר אל מול רשתות יעד ותשתיות ארגוני טרור", הדגיש, "אנחנו חיים בסביבה קשה, וזה מצריך מאיתנו לעבוד קשה, בסביבה דינמית ואינטנסיבית, שמספקת אתגרים חדשים מדי יום. כשאנחנו מצליחים אנחנו מצילים חיים. כשאנחנו נכשלים זה הופך לבעיה גדולה עבור האומה שלנו". הוא סיפק מידע על פעילות היחידה, וציין כי היא מהווה חלק מרכזי במערך המודיעין וההגנה של ישראל. "אנחנו עובדים בשיתוף פעולה עם היחידות האחרות, כאשר סיכול איומי סייבר הוא חלק מרכזי בפעילות שלנו", הדגיש סגן מפקד יחידת 8200, "מטרתנו היא להשיג עליונות על התוקף, להצליח לזהות אותו ולפעול כדי לשלול את יכולותיו. כך לעיתים אנו גם מוצאים קורבנות מחוץ לישראל ואז אנו יוצרים קשר עם סוכניות אחרות אם צריך". לדבריו, אנו עושים זאת גם באופן עצמאי וגם על ידי שיתוף פעולה עם התעשייה וסוכנויות אחרות, באמצעות יישום ושימוש בכלים שפיתחנו, 8200 לא תנוח עד שהאיום יוסר.

אורי חשף כי היחידה סיכלה לפני מספר שנים "ניסיון להשתלט על מערכות המים הקריטיות של ישראל, ולרעיל אותן. במקרה אחר, זיהינו גם כי יריב מסוים תקף את ישראל ותוך כדי זיהינו שאותו תוקף ניסה גם לכוון לתחנות כוח בארה"ב". לדבריו, במקרה זה, מדובר היה באינדיקציה הראשונה להתקפה זו. "את האיום הזה הצלחנו למנוע באמצעות שיתוף פעולה הדוק עם השותפים האמריקאים שלנו. הישגים כאלו הם שגורמים לחיילים שלנו להיות גאים בעבודתם ב-8200", ציין.

"רוב מה שאנחנו עושים חסוי, ואנחנו פועלים על מנת למנוע איומי סייבר נגד ישראל ומבטיחים שישראל תישאר מעצמה מובילה בתחום הטכנולוגיה והסייבר באזורנו", סיכם, "בתוך המרחב הזה, יש לנו אחריות על אתיקה, מוסר וערכים ואנו לוקחים אותה ברצינות רבה, תוך שמירת מחויבות לערכים הדמוקרטיים שלנו, לנורמות במרחב הסייבר, ולחברה הישראלית וזו הסיבה העיקרית שאני עומד פה היום".

מעריב

"במטרה לפגוע בלבנון": גנץ חשף פעילות משותפת של איראן וחיזבאללה

שר הביטחון התייחס בנאום באוניברסיטת ת"א לסרטון שפרסם חמאס, וחשף כי "כוחות הביטחון האיראנים וחיזבאללה ניסו לפגוע בפעילות כוחות יוניפי"ל בלבנון"

אנה ברסקי

שר הביטחון בני גנץ התייחס הבוקר (חמישי) במהלך נאום שנשא בשבוע הסייבר השנתי, בהובלת המרכז למחקר סייבר באוניברסיטת ת"א, מערך הסייבר הלאומי, משרד הכלכלה ומשרד החוץ, להתפתחויות האחרונות בחזית הביטחונית. בראשית דבריו, הגיב לסרטון שפרסם אמש ארגון חמאס, בו נראה השבוי הישראלי הישאם א-סייד כשהוא מחובר למכשיר חמצן: "מטרת הסרטון היא סחטנות על גבה של סוגייה הומניטרית".

הוא המשיך ותקף את ארגון הטרור: "חמאס מחזיק בשבי במשך שנים את ארבעת הבנים, זאת בניגוד לחוק הבינלאומי והמוסר. בחמאס אחראים לכך, והציפייה שלנו מהקהילה הבינלאומית היא לפעול מול ההתנהלות הנפשעת שלהם". גנץ הוסיף כי "מדינת ישראל פועלת במגוון אמצעים, וממשיכה להפוך על אבן על מנת להשיב את הבנים הביתה. כפי שאמרנו בעבר - מדובר בסוגייה הומניטרית, כך אנחנו רואים אותה ועל הבסיס הזה נמשיך לפעול". הוא הדגיש עוד כי "ניסיונות סחטנות ותרגילי תודעה לא ישפיעו על התנהלותנו". בהמשך הנאום, הוא התייחס לסוגייה האיראנית וציין כי "איראן מפעילה את שלוחיה גם במימד הסייבר. אני יכול לחשוף היום, שלאחרונה אותרה פעילות של גופי הביטחון האיראנים בשיתוף עם חיזבאללה, בכדי לפגוע בפעילות כוחות יוניפי"ל בלבנון. זאת על ידי מימוש מבצע בסייבר שמטרתו הייתה לגנוב חומרים על היערכות יוניפ"ל במרחב, ושימוש בהם על ידי חיזבאללה". לדבריו, זוהי פגיעה נוספת של איראן וחיזבאללה באזרחי לבנון, וביציבותה של לבנון.

"ישראל מכירה את מערכות הסייבר של יריביה ואת דרכי הפעולה שלהם", הדגיש שר הביטחון, "אנו רואים בשנים האחרונות תופעה של קבוצות האקרים מטעם איראן, שפועלות מול ישראל ומדינות נוספות. <השלוחים החדשים>, הם טרוריסטים עם מקלדת שדינם כמו לוחמי ארגוני טרור אחרים. אנחנו יודעים מי הם, אנחנו פוגעים בהם ובשולחיהם, וגם היום הם על הכוונת שלנו – ולא רק במימד הקיברנטי".

גנץ הדגיש: "שום מתקפה מול אזרחי ישראל לא תעבור לסדר היום. האחריות היא של התוקפים ושל המדינה שממממנת ושולחת אותם. תקיפת סייבר יכולה להיענות במגוון דרכים במרחב הסייבר ובמרחבים נוספים. איראן מובילה את טרור הסייבר – ועושה מהלכים שמטרתם להשפיע על תהליכים דמוקרטיים ועל ממשלים, כפי שקרה בבחירות לנשיאות ארצות הברית ובניסיונות נוספים שישראל מודעת אליהם".

לדבריו, פעולות כמו זו של יחידת "שאהיד כאווה" שאספה מידע על ספינות, תחנות דלק ומפעלי תעשייה במספר מדינות, נעשו תחת דירקטיבה ישירה של ההנהגה האיראנית ומשמרות המהפכה כפי שנחשף בתחקירים. "בשנים האחרונות בלמנו ניסיונות רבים לפרוץ לחברות פרטיות וציבוריות, בארץ ובחו"ל. אני קורא גם לציבור לדרוש <אחריות קיברנטית>, ולהעניש חברות וגופים שלא פועלים בהתאם להנחיות", הוסיף.

"המשימה העליונה שלנו, בצבא, בתעשיות ובארגוני הביטחון השונים היא לבנות את האנשים, להכשיר אותם, ולהשאיר אותם. אני והרמטכ"ל הצבנו את הנושא הזה כאחת המשימות המרכזיות ביחידות הרלוונטיות. אנחנו בוחנים את בניין הכוח כל העת – גם בהיקפי כוח האדם, גם בנושא ההכשרות וגם בנושא המשימות", הדגיש, "בשנים הקרובות נצטרך גם לבחון את צורת ההתארגנות, הניהול והתפעול של לוחמת הסייבר, על מאפייניה ההתקפיים וההגנתיים בצה"ל ובמערכת הביטחון כולה".

הוא סיכם: "יש חשיבות גדולה לשיתופי הפעולה שלנו עם העולם מול איראן גם במימד הסייבר. את אותם שיתופי פעולה שאנו בונים באזור מול איראן בהיבטים של הגנה מול איומים שונים – אנחנו מרחיבים גם במימד הסייבר".

מעריב

» מתקפת סייבר

קבוצת Sharp Boys: "פרצנו לאתרי תיירות ישראליים"

ההאקרים טוענים שביצעו מתקפת מניעת שירות על האתר hotel4u ■ הם פרסמו כ־140 אלף רשומות עם פרטים אישיים של ישראלים, נוסף ל־200 מספרי כרטיסי אשראי ■ ראש מערך הסייבר: "איראן הפכה לשחקן מרכזי במרחב הסייבר יחד עם חמאס וחיזבאללה"

מתן וסרמן

קבוצת תקיפה בשם Sharp Boys, שפעילה בזמן האחרון נגד מטרות ישראליות, טוענת שהצליחה לפרוץ לאתרי תיירות ישראליים. במקביל, ההאקרים טוענים כי ביצעו מתקפת מניעת שירות (DDOS) על האתר hotel4u.

בערוץ הטלגרם של התוקפים פורסם מאגר של כ־140 אלף רשומות עם פרטים אישיים של ישראלים, שמות, אי־מיילים ומספרי טלפון, נוסף ל־200 מספרי כרטיס אשראי. זו הפעם השנייה שהקבוצה תוקפת את hotel4u, ולא ברור אם מקור התוקפים באיראן.

"גלי תקיפת הסייבר על מטרות אזרחיות ישראליות המשכים. מובן שברגע שהתוקפים מצליחים לשים את ידם על מאגרי מידע של החברות המותקפות האפקט התודעתי הוא משמעותי", אומר עודד ואנונו, ראש מחקר חולשות מוצרים בצ'ק פוינט.

"כתוצאה מכך אזרחים שפרטיהם נחשפו צריכים להיות יותר ערניים ולשקול לאפס סיסמאות ולהפעיל אימות דו־שלבי על האפליקציות החשובות כמו אפליקציות מייל, רשתות חברתיות ובנקים"

בנאום מקיף ראשון מאז כניסתו לתפקיד לפני כארבעה חודשים הציג אתמול ראש מערך הסייבר הלאומי גבי פורטנוי את הפרויקט החדש של המערך ליצירת כיפת סייבר על המרחב האזרחי.

בהתייחס לתוקפים במרחב אמר פורטנוי: "איראן הפכה לשחקן מרכזי שאנחנו מזהים במרחב הסייבר יחד עם חמאס וחיזבאללה. אנחנו רואים אותם, אנחנו יודעים איך הם עובדים ואנחנו שם".

ורגע לפני סיום כהונתו, ראש הממשלה נפתלי בנט השתתף אתמול בכנס הסייבר העולמי באוניברסיטת תל אביב, והתייחס לאיומי הסייבר על ישראל מצד איראן ולדרך הפעולה של ישראל בנדון.

"הייתי מופתע מחוסר השימוש בכלי הסייבר במלחמה באוקראינה", אמר בנט בפתח דבריו, "חשבתי שזה יהיה שימוש מתקדם יותר וזה לא קרה. אם אפשר להשיג את אפקט המלחמה דרך הסייבר ולא לסכן חיי אדם, זה מה שצריך לעשות ברמה הפוליטית".

N12 החדשות

בן מיטלמן

מבקר המדינה מתניהו אנגלמן בשבוע הסייבר באוניברסיטת ת"א עם ביקורת קשה בנוגע למוכנות הגנת הסייבר: "לאזרחי העולם אין הגנה. הנתונים שלנו גלויים ליותר מדי אנשים. הביטחון שלנו חשוף. מלחמת העולם השלישית תהיה מלחמת סייבר, אבל העולם לא מוכן אליה"

ניר דבורי

סגן מפקד יחידת 8200 בשבוע הסייבר השנתי באוניברסיטת ת"א: היחידה סיכלה להשתלט על מערכות המים הקריטיות של ישראל והתריעה על תוקפים שניסו לפגוע בתחנות כוח בארה"ב

11:05

ניר דבורי

שר הביטחון גנץ התייחס בכנס הסייבר באוניברסיטת תל אביב לסרטון שפרסם חמאס שבו נראה השבוי הישראלי הישאם א-סייד: "ניסיונות סחטנות ותרגילי תודעה לא ישפיעו על התנהלותנו"

12:09

ice.

מבקר המדינה: "ליקויים במוכנות ועדת הבחירות למתקפות סייבר"

מבקר המדינה מתניהו אלגמן מזהיר כי לא בוצעו בדיקות מקיפות למוכנות מערכות המחשוב של ועדת הבחירות למתקפות סייבר: "ביקורות נערכו רק בתקופות בחירות, כך שלא ניתן היה לבצע בדיקות מקיפות ומורכבות "

מבקר המדינה מתניהו אנגלמן השתתף היום (רביעי) בשבוע הסייבר השנתי של אוניברסיטת תל אביב ונתן סקירה מקיפה, על ביקורת הסייבר אותה הוא מבצע מאז כניסתו לתפקיד.

"הסייבר היום חשוב מתמיד", פתח אנגלמן. "במובן מסוים, כולנו חיים בתוך תכנית <האח הגדול> בינלאומית. כמבקר מדינת ישראל אני חייב לחלוק איתכם אמירה פסימית: אנחנו חשופים. לאזרחי העולם אין הגנה. הנתונים שלנו גלויים ליותר מדי אנשים. הכסף שלנו חשוף, הילדים שלנו חשופים, הבריאות שלנו חשופה, הביטחון שלנו חשוף. מלחמת העולם השלישית תהיה מלחמת סייבר, אבל העולם לא מוכן אליה" אמר.

מארגני הכנס דיווחו שאלגמן אף הצהיר כי "עלו ליקויים משמעותיים במוכנות ועדת הבחירות המרכזית לאיומי הסייבר". לדבריו," דו"ח על מערכת המחשוב של ועדת הבחירות המרכזית בישראל מצא כי מערכת המחשוב המרכזית שלהם החלה לפעול בשנת 2008 והיא חגגה <בר מצווה> בשנה שעברה. ועדיין, ביקורות סייבר נערכו רק בתקופות בחירות, כך שלא ניתן היה לבצע בדיקות מקיפות ומורכבות שכללו את כל ההיבטים הנדרשים להגנת הסייבר".

הוא הוסיף כי בשנה האחרונה נמצאו ליקויים משמעותיים בביקורת חדירה שבוצעה במספר גופים ציבורים, בהם: מרכז ניהול התנועה בירושלים, מערכות רשות המיסים ובתי החולים. "מעט מאוד בדיקות חדירה בוצעו על ידי גופים ציבוריים וחלקם ערכו בדיקות חדירה רק במהלך הביקורת", ציין.

ערוץ 7 www.inn.co.il

מצב הסייבר ישראל: "אנחנו חשופים, נטולי הגנה"

מבקר המדינה מתניהו אנגלמן מודה: "יש ליקויים משמעותיים במוכנות ועדת הבחירות המרכזית לאיומי הסייבר".

מבקר המדינה מתניהו אנגלמן השתתף היום (רביעי) בכנס הסייבר השנתי של אוניברסיטת תל אביב ונתן סקירה מקיפה על ביקורת הסייבר אותה הוא מבצע החל מכניסתו לתפקיד.

"הסייבר היום חשוב מתמיד", פתח אנגלמן. "במובן מסוים, כולנו חיים בתוך תכנית <האח הגדול> בינלאומית. כמבקר מדינת ישראל וסגן נשיא EUROSAI, אני חייב לחלוק איתכם אמירה פסימית: אנחנו חשופים. לאזרחי העולם אין הגנה. הנתונים שלנו גלויים ליותר מדי אנשים. הכסף שלנו חשוף, הילדים שלנו חשופים, הבריאות שלנו חשופה, הביטחון שלנו חשוף. מלחמת העולם השלישית תהיה מלחמת סייבר, אבל העולם לא מוכן אליה".

לדבריו, "עם כניסתי לתפקיד הנוכחי של מבקר המדינה, ולנוכח איומי הסייבר ההולכים וגדלים איתם מתמודדת מדינת ישראל בשנים האחרונות, החלטתי להציב את תחום הסייבר כאחד מבעיות הליבה בהן תעסוק הביקורת. הוקמו חטיבת ביקורת סייבר וחטיבה ייעודית לביקורת מערכות מידע. בהתחלה היו כאלה ש>הרימו גבה<. היום אין מי שלא מבין את חשיבות הנושא. גם ארגון המבקרים הבינלאומי קבע כי הגנה כזו על מערכות מידע היא אחד הסיכונים הגדולים ביותר".

אנגלמן סיפר כי במסגרת ביקורות הסייבר הוא בודק את הגנת הפרטיות, מנגנוני בקרה והגנה של המערכות הממוחשבות; השקעה ב-IT, היערכות מוקדמת לאירועי סייבר והתאוששות מאסון, התקפות סייבר ופגיעה בתשתיות מדינה קריטיות. ועוד. כמו כן, הוא הנחה לקיים מבחני חדירה על ידי חברות האקרים מטעם משרד מבקר המדינה.

"דו"ח על מערכת המחשוב של ועדת הבחירות המרכזית בישראל מצא כי מערכת המחשוב המרכזית שלהם החלה לפעול בשנת 2008 והיא חגגה <בר מצווה> בשנה שעברה. ועדיין, ביקורות סייבר נערכו רק בתקופות בחירות, כך שלא ניתן היה לבצע בדיקות מקיפות ומורכבות שכללו את כל ההיבטים הנדרשים להגנת הסייבר".

"בשנה האחרונה ביצענו בדיקות חדירה במרכז ניהול התנועה בירושלים, בבתי חולים ובמערכות רשות המסים. בביקורות מצאנו ליקויים משמעותיים, לרבות העובדה שמעט מאוד בדיקות חדירה בוצעו על ידי גופים ציבוריים וחלקם ערכו בדיקות חדירה רק במהלך הביקורת; אנו במשרד מבקר המדינה מתחייבים להמשיך ולהתייחס לנושא משמעותי זה ביתר שאת, לטובת אזרחי ישראל והעולם כולו", סיכם.

PC אנשים ומחשבים

"איראן וחיזבאללה פגעו בסייבר בפעילות יוניפי"ל בלבנון"

כך סיפר היום (ד>) שר הביטחון, בני גנץ, במהלך נאום שנשא במסגרת כנס הסייבר הבינלאומי של מרכז הסייבר באוניברסיטת ת"א "השלוחים החדשים הם טרוריסטים עם מקלדת, שדינם כמו לוחמי ארגוני טרור אחרים", אמר

שר הביטחון, בני גנץ, נאם היום (ד>) במסגרת כנס הסייבר הבינלאומי של מרכז הסייבר באוניברסיטת ת"א.

בין השאר סיפר גנץ בנאומו כי "איראן מפעילה את שלוחיה גם בממד הסייבר: אני יכול לחשוף היום, שלאחרונה אותרה פעילות של גופי הביטחון האיראנים בשיתוף עם חיזבאללה, בכדי לפגוע בפעילות כוחות יוניפי"ל בלבנון. זאת על ידי מימוש מבצע בסייבר, שמטרתו הייתה לגנוב חומרים על היערכות יוניפ"ל במרחב, ושימוש בהם על ידי חיזבאללה. זוהי פגיעה נוספת של איראן וחיזבאללה באזרחי לבנון וביציבותה של לבנון".

גנץ הדגיש בדבריו ש-"ישראל מכירה את מערכות הסייבר של יריביה ואת דרכי הפעולה שלהם. אנו רואים בשנים האחרונות תופעה של קבוצות האקרים מטעם איראן, שפועלות מול ישראל ומדינות נוספות".

"השלוחים החדשים", המשיך והרחיב גנץ, "הם טרוריסטים עם מקלדת, שדינם כמו לוחמי ארגוני טרור אחרים. אנחנו יודעים מי הם, אנחנו פוגעים בהם ובשולחיהם, וגם היום הם על הכוונת שלנו – ולא רק בממד הקיברנטי. שום מתקפה מול אזרחי ישראל לא תעבור לסדר היום, והאחריות היא של התוקפים ושל המדינה שממנת ושולחת אותם. תקיפת סייבר יכולה להיענות במגוון דרכים במרחב הסייבר ובמרחבים נוספים".

עוד לדברי גנץ: "איראן מובילה את טרור הסייבר – ועושה מהלכים שמטרתם להשפיע על תהליכים דמוקרטיים ועל ממשלים, כפי שקרה בבחירות לנשיאות ארצות הברית ובניסיונות נוספים שישראל מודעת אליהם. פעולות כמו זו של יחידת <שאהיד כאווה>, שאספה מידע על ספינות, תחנות דלק ומפעלי תעשייה במספר מדינות, נעשו תחת דירקטיבה ישירה של ההנהגה האיראנית ומשמרות המהפכה, כפי שנחשף בתחקירים".

קרא לציבור להפגין "אחריות קיברנטית"

"בשנים האחרונות בלמנו ניסיונות רבים לפרוץ לחברות פרטיות וציבוריות, בארץ ובחו"ל", סיפר גנץ. "אני קורא גם לציבור לדרוש <אחריות קיברנטית>, ולהעניש חברות וגופים שלא פועלים בהתאם להנחיות".

גנץ התייחס גם לכוח הפעולה הישראלי בגזרת הסייבר והסביר: "המשימה העליונה שלנו, בצבא, בתעשיות ובארגוני הביטחון השונים היא לבנות את האנשים, להכשיר אותם, ולהשאיר אותם. אני והרמטכ"ל הצבנו את הנושא הזה כאחת המשימות המרכזיות ביחידות הרלבנטיות. אנחנו בוחנים את בניין הכוח כל העת – גם בהיקפי כוח האדם, גם בנושא ההכשרות וגם בנושא המשימות. בשנים הקרובות נצטרך גם לבחון את צורת ההתארגנות, הניהול והתפעול של לוחמת הסייבר, על מאפייניה ההתקפיים וההגנתיים בצה"ל ובמערכת הביטחון כולה".

גנץ סיכם ואמר כי "יש חשיבות גדולה לשיתופי הפעולה שלנו עם העולם מול איראן גם בממד הסייבר. את אותם שיתופי פעולה שאנו בונים באזור מול איראן, בהיבטים של הגנה מול איומים שונים – אנחנו מרחיבים גם בממד הסייבר".

Instagram

News1 מחלקה ראשונה

אנגלמן על מצב הסייבר בישראל: "אנחנו חשופים, נטולי הגנה"

הזהיר: "עלו ליקויים משמעותיים במוכנות ועדת הבחירות המרכזית לאיומי הסייבר" הוסיף: "מלחמת העולם השלישית תהיה מלחמת סייבר אך העולם לא ערוך אליה" "בדיקות חדירה שביצענו העלו ליקויים רבים"

מירב ארד

בקר המדינה מתניהו אנגלמן השתתף (יום ד', 29.6.22) בכנס הסייבר השנתי של אוניברסיטת תל אביב ונתן סקירה מקיפה, לראשונה, על ביקורת הסייבר אותה הוא מבצע החל מכניסתו לתפקיד - אז הקים אגף סייבר מיוחד.

"הסייבר היום חשוב מתמיד", פתח אנגלמן. "במובן מסוים, כולנו חיים בתוך תוכנית <האח הגדול> בינלאומית. כמבקר מדינת ישראל וסגן נשיא EUROSAI, אני חייב לחלוק איתכם אמירה פסימית: אנחנו חשופים. לאזרחי העולם אין הגנה. הנתונים שלנו גלויים ליותר מדי אנשים. הכסף שלנו חשוף, הילדים שלנו חשופים, הבריאות שלנו חשופה, הביטחון שלנו חשוף. מלחמת העולם השלישית תהיה מלחמת סייבר, אבל העולם לא מוכן אליה.

עם כניסתי לתפקיד הנוכחי של מבקר המדינה, ולנוכח איומי הסייבר ההולכים וגדלים איתם מתמודדת מדינת ישראל בשנים האחרונות, החלטתי להציב את תחום הסייבר כאחד מבעיות הליבה בהן תעסוק הביקורת. הוקמו חטיבת ביקורת סייבר וחטיבה ייעודית לביקורת מערכות מידע. בהתחלה היו כאלה ש>הרימו גבה<. היום אין מי שלא מבין את חשיבות הנושא. גם ארגון המבקרים הבינלאומי קבע כי הגנה כזו על מערכות מידע היא אחד הסיכונים הגדולים ביותר".

אנגלמן סיפר כי במסגרת ביקורות הסייבר הוא בודק את הגנת הפרטיות, מנגנוני בקרה והגנה של המערכות הממוחשבות; השקעה ב-IT, היערכות מוקדמת לאירועי סייבר והתאוששות מאסון, התקפות סייבר ופגיעה בתשתיות מדינה קריטיות. ועוד. כמו-כן, הוא הנחה לקיים מבחני חדירה על-ידי חברות האקרים מטעם משרד מבקר המדינה.

"דוח על מערכת המחשוב של ועדת הבחירות המרכזית בישראל מצא כי מערכת המחשוב המרכזית שלהם החלה לפעול בשנת 2008 והיא חגגה "בר מצווה" בשנה שעברה. ועדיין, ביקורות סייבר נערכו רק בתקופות בחירות, כך שלא ניתן היה לבצע בדיקות מקיפות ומורכבות שכללו את כל ההיבטים הנדרשים להגנת הסייבר.

בשנה האחרונה ביצענו בדיקות חדירה במרכז ניהול התנועה בירושלים, בבתי חולים ובמערכות רשות המיסים. בביקורות מצאנו ליקויים משמעותיים, לרבות העובדה שמעט מאוד בדיקות חדירה בוצעו על-ידי גופים ציבוריים וחלקם ערכו בדיקות חדירה רק במהלך הביקורת; אנו במשרד מבקר המדינה מתחייבים להמשיך ולהתייחס לנושא משמעותי זה ביתר שאת, לטובת אזרחי ישראל והעולם כולו".

PC אנשים ומחשבים

בנט: "אויב שיתקוף אותנו בסייבר – יחטוף"

יום לפני שהוא עוזב את כיסא ראש הממשלה, נפתלי בנט שחרר הצהרות לוחמניות נגד איראן - גם בסייבר● "אתם לא יכולים יותר להכות בישראל באופן לא ישיר, גם בסייבר, ולחשוב שתתחמקו מאתנו", אמר ראש הממשלה לאויבינו

יניב הלפרין

ראש הממשלה, נפתלי בנט, שחרר היום (ג') הצהרות לוחמניות במיוחד נגד איראן ופעילותה נגד ישראל במרחב הסייבר. לדברי בנט, "אני אומר לאויבים שלנו, ובמיוחד לאיראן: אם אתם מתעסקים עם ישראל – תשלמו מחיר. בסייבר כמו בממד הפיזי, אתם לא יכולים יותר להכות בישראל באופן לא ישיר, דרך החמאס או החיזבאללה, ולחשוב שתתחמקו מאתנו. אתם הבריון ששולחים אנשים אלינו, ונילחם בכם יותר מאשר בשליחים שלכם. מי שיתקיף אותנו בסייבר – נתקוף אותו בחזרה".

דבריו של בנט מגיעים יום לאחר שהתחוללה מתקפת סייבר על מפעל פלדה באיראן, שמתנגדי משטר מיהרו לקחת עליה אחריות, אם כי גם שמה של ישראל עולה בהקשר זה, ובכלל, מלחמת הסייבר המתמשכת בינה לבין ישראל. האחרון בשרשרת האירועים שבאופן ודאי הם חלק מהמלחמה הזאת הוא המתקפה שגורמים איראניים ביצעו בשבוע שעבר, שגרמה להפעלת אזעקות שוא בירושלים ובאילת, ויוחסה לאיראן.

יום לפני שהוא, כפי שמסתמן, עוזב את תפקיד ראש הממשלה, בנט השתתף הבוקר בשבוע הסייבר של אוניברסיטת תל אביב. הוא אמר את הדברים בשיחה שניהל עם מיכל ברוורמן בלומנשטיק, מנכ"לית מיקרוסופט ישראל מחקר ופיתוח וסמנכ"לית טכנולוגיות הענן והבינה המלאכותית של חברת הענק. השניים סגרו מעגל, לאחר שהיו ביחד בין מייסדי סאיוטה, שבנט היה גם המנכ"ל שלה. בשיחה הם דנו על פוליטיקה ועל סייבר כאחד.

בנט עמד על לוחמת הסייבר מול הלוחמה הפיזית: "כיום אפשר לנצח את האויב בסייבר, עם קבוצה של אנשים שיושבת

מאחורי מקלדת במקום 50 או 100 חיילי קומנדו מאחורי קווי האויב. הסייבר עומד להיות אחד הממדים הדומיננטיים של לוחמת העתיד, אם לא הדומיננטי שבהם".

"הופתעתי מכך שהיה שימוש מועט בסייבר, לפחות עד עכשיו, במלחמת רוסיה-אוקראינה. חשבתי שיהיה יותר שימוש בהם, ושימוש מתקדם. אבל זאת לא דוגמה, משום שמתקפות הסייבר הולכות וגוברות, ומשתכללות, והמגמה הזאת תמשיך. בלוחמת סייבר כמו בפשעי הסייבר, הוא לא רק שיישאר, אלא יהיה גרוע יותר", אמר בנט.

אחד הפתרונות המרכזיים לכך, לדברי ראש הממשלה, הוא שיתופי פעולה בין ממשלות, ובינן לבין תעשיות ההיי-טק והסייבר. "שיתוף פעולה בינלאומי חיוני בסייבר, כי קבוצת האקרים שתוקפת מדינה אחת תוקפת באותו הזמן, או בזמן סמוך, עוד מדינות, ואם הן חולקות מידע – כולן יכולות להגן על עצמן. אנחנו בונים רשת של שיתופי פעולה עם ארצות הברית, בריטניה ומדינות אחרות, ונמשיך בכך. אם לא נעבוד ביחד, העולם יהפוך לסיוט של סייבר. אנחנו צריכים להילחם ביחד באויבי הסייבר – ואני אופטימי", ציין.

"הממשלה וההיי-טק כמעט הפוכים"

בנט ציין כי אחת המשימות הלאומיות החשובות ביותר היא לשלב את החרדים, הערבים – ובמיוחד הנשים הערביות – והפריפריה בתעשיית ההיי-טק. "הגברים החרדים חכמים, אבל הם לא חלק מהכלכלה הישראלית. הם בעלי אינטליגנציה גבוהה, אבל במקרה הטוב יש להם ידע בסיסי", אמר. "התחלנו תוכנית להכשרת החכמים שבחכמים שבגברים החרדים להיי-טק, עם לימודי אנגלית ומתמטיקה, ואני אופטימי". "עוד מקור הוא נשים ערביות. הן פחות מועסקות באופן כללי, והמשימה היא להביא אותן לעבודה, כולל להיי-טק. מקורות נוספים הם הפריפריה והעובדים הפלסטינים. זה דורש מקהילת ההיי-טק להיות פתוחה לאנשים שהם לא מאותו המועדון. יש גם את אנשי ההיי-טק הישראלים שעובדים בחו"ל, שאני קורא להם לשוב הביתה", ציין.

לדברי בנט, "השיעור הראשון שלמדתי בתקופתי כראש ממשלה הוא שכמו במגזר הפרטי, צריכים לזוז מהר, להראות תוצאות מהר וליצור תחושה של הצלחה. המידע חיוני לצורך כך, והפוליטיקה וההיי-טק כמעט הפוכים בהקשר זה, כי בממשלה, אתה מאבד מידע במעלה ההיררכיה, משום שלא אוהבים לתת לך חדשות רעות. לכן, אני אוהב לעקוף את ההיררכיה. למשל, לפגוש קצינים צעירים אם אני חש שיש משהו לא טוב בצבא, או לפגוש מורים מתחילים".

כיפה

מבקר המדינה חושש מאיומי הסייבר: "אנחנו חיים בתוך תכנית עולמית של 'האח הגדול'"

מבקר המדינה העלה תמונת מצב קודרת בכל הקשור לאיומי הסייבר על ישראל ואמר, "אנחנו חשופים, נטולי הגנה", וחושש לפגיעה בטוהר הבחירות "עלו ליקויים משמעותיים במוכנות ועדת הבחירות המרכזית לאיומי הסייבר"

מבקר המדינה מתניהו אנגלמן השתתף היום (ד<) בכנס הסייבר השנתי של אוניברסיטת תל אביב ונתן סקירה מקיפה, לראשונה, על ביקורת הסייבר אותה הוא מבצע החל מכניסתו לתפקיד – אז הקים אגף סייבר מיוחד.

"הסייבר היום חשוב מתמיד", פתח אנגלמן. "במובן מסוים, כולנו חיים בתוך תכנית <האח הגדול> בינלאומית. כמבקר מדינת ישראל וסגן נשיא EUROSAI, אני חייב לחלוק איתכם אמירה פסימית: אנחנו חשופים. לאזרחי העולם אין הגנה. הנתונים שלנו גלויים ליותר מדי אנשים. הכסף שלנו חשוף, הילדים שלנו חשופים, הבריאות שלנו חשופה, הביטחון שלנו חשוף. מלחמת העולם השלישית תהיה מלחמת סייבר, אבל העולם לא מוכן אליה.

אנגלמן: "החלטתי להציב את תחום הסייבר כאחד מבעיות הליבה בהן תעסוק הביקורת"

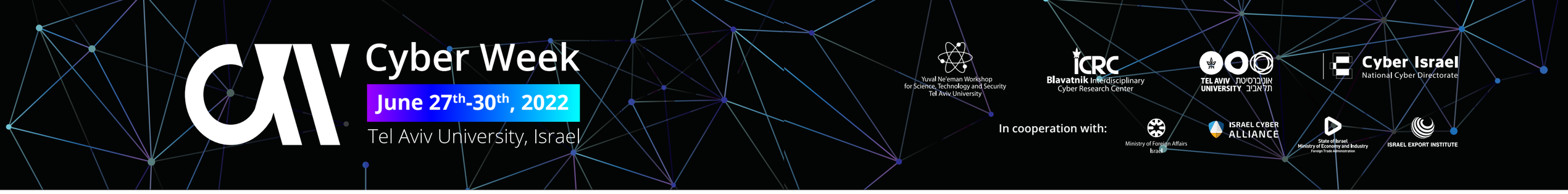
עם כניסתי לתפקיד הנוכחי של מבקר המדינה, ולנוכח איומי הסייבר ההולכים וגדלים איתם מתמודדת מדינת ישראל בשנים האחרונות, החלטתי להציב את תחום הסייבר כאחד מבעיות הליבה בהן תעסוק הביקורת. הוקמו חטיבת ביקורת סייבר וחטיבה ייעודית לביקורת מערכות מידע. בהתחלה היו כאלה ש>הרימו גבה<. היום אין מי שלא מבין את חשיבות הנושא. גם ארגון המבקרים הבינלאומי קבע כי הגנה כזו על מערכות מידע היא אחד הסיכונים הגדולים ביותר".

אנגלמן סיפר כי במסגרת ביקורות הסייבר הוא בודק את הגנת הפרטיות, מנגנוני בקרה והגנה של המערכות הממוחשבות; השקעה ב-IT, היערכות מוקדמת לאירועי סייבר והתאוששות מאסון, התקפות סייבר ופגיעה בתשתיות מדינה קריטיות. ועוד. כמו כן, הוא הנחה לקיים מבחני חדירה על ידי חברות האקרים מטעם משרד מבקר המדינה.

ביצענו בדיקות חדירה במרכז ניהול התנועה בירושלים, בבתי חולים ובמערכות רשות המסים - מצאנו ליקויים משמעותיים

"דו"ח על מערכת המחשוב של ועדת הבחירות המרכזית בישראל מצא כי מערכת המחשוב המרכזית שלהם החלה לפעול בשנת 2008 והיא חגגה "בר מצווה" בשנה שעברה. ועדיין, ביקורות סייבר נערכו רק בתקופות בחירות, כך שלא ניתן היה לבצע בדיקות מקיפות ומורכבות שכללו את כל ההיבטים הנדרשים להגנת הסייבר.

בשנה האחרונה ביצענו בדיקות חדירה במרכז ניהול התנועה בירושלים, בבתי חולים ובמערכות רשות המסים. בביקורות מצאנו ליקויים משמעותיים, לרבות העובדה שמעט מאוד בדיקות חדירה בוצעו על ידי גופים ציבוריים וחלקם ערכו בדיקות חדירה רק במהלך הביקורת; אנו במשרד מבקר המדינה מתחייבים להמשיך ולהתייחס לנושא משמעותי זה ביתר שאת, לטובת אזרחי ישראל והעולם כולו".



כאן

יועצת הסייבר החרדית של הנשיא ביידן בריאיון בלעדי

אן נויברגר, יהודייה חרדית אמריקנית, מתמודדת בתפקידה במועצה לביטחון לאומי עם האיומים הטכנולוגיים על אמריקה. היא אחראית לשיתופי הפעולה עם מדינות אחרות בתחום. בריאיון בלעדי לכאן חדשות היא מספרת על החשש מהאיום האיראני, ומהאפשרות שרוסיה שוב תתערב בבחירות

כמו בישראל, גם הממשל בוושינגטון מודאג יותר ויותר בימים אלו מהיכולות האיראניות, במיוחד בתחום מתקפות הסייבר. אחת מהאנשים שמייעצים לנשיא ארצות הברית באותו נושא, היא אן נויברגר החרדית, סגנית היועץ לביטחון לאומי האמריקני לענייני סייבר.

"איראן ומדינות נוספות, הופכים להיות טובים יותר בעולם הסייבר". מספרת נויברגר. "אנחנו רואים התגברות בסוגים שונים של איומי סייבר מצד איראן, וגם לדוגמה איומי כופרה וגם על איומים נגד מדינות. רק השבוע חשף שר הביטחון גנץ כי ישראל סייעה לארצות הברית במניעת מתקפת סייבר נגד תחנות כוח, ולנויברגר, שהגיעה לישראל במסגרת סייבר וויק של אוניברסיטת תל אביב, חשוב להדגיש את שיתוף הפעולה הזה.

הסיפור של נויברגר, יכול להכיל כתבה בפני עצמה. סבה וסבתה הם ניצולי שואה, והוריה חסידי סאטמר. היא עצמה דוברת עברית, ערבית וגם יידיש, מקיימת אורח חיים חרדי מלא, ופועלת בשנים האחרונות למען שילובן של נשים וקבוצות מיעוט בתחום הסייבר. ברזומה שלה תוכלו למצוא קריירה ארוכה בפנטגון ובנושאי סייבר בממשל – והיא עוסקת לא מעט בחשש מהתעצמות סין.

כלכליסט

ועדת הבחירות המרכזית מגיבה לדברי המבקר: מעודד התקפות סייבר עלינו

מבקר המדינה מתניהו אנגלמן האשים מוקדם יותר היום את הוועדה ב"ליקויים משמעותיים בהכנה לאיומי סייבר". הוועדה טוענת בתגובה ש"שיח סייבר בכיכר העיר מעודד כל תוקף פוטנציאלי"

שחר אילן

ועדת הבחירות המרכזית מאשימה את מבקר המדינה מתניהו אנגלמן בעידוד התקפות סייבר עליה. הדברים נאמרו בתגובה לנאומו של המבקר היום (רביעי) בו אמר ש"עלו ליקויים משמעותיים במוכנות ועדת הבחירות המרכזית לאיומי הסייבר". הוא הביא את ועדת הבחירות כדוגמה לגוף שיש שאינו מודע לחובתו לשמור על מערכות המחשוב.

המבקר דיבר בשבוע הסייבר הבינלאומי של אוניברסיטת תל אביב. הוא טען ש"מלחמת העולם השלישית תהיה מלחמת סייבר אך העולם לא ערוך אליה". הוא סקר את הפעילות שלו בתחום ביקורת הסייבר ובין היתר אמר ש"יש מחסור במודעות של גופים ציבוריים לחובתם להגן על מערכות המחשב שלהם. למשל דו"ח על מערכת המחשוב של ועדת הבחירות המרכזית בישראל מצא כי מערכת המחשוב המרכזית שלהם החלה לפעול בשנת 2008 והיא חגגה "בר מצווה" בשנה שעברה. ועדיין, ביקורות סייבר נערכו רק בתקופות בחירות, כך שלא ניתן היה לבצע בדיקות מקיפות ומורכבות שכללו את כל ההיבטים הנדרשים להגנת הסייבר".

הוועדה בתגובה פרסמה הודעה כי היא "דוחה מכל וכל את אמירת המבקר לפיה אינה ערוכה לאיומי סייבר". לטענת ועדת הבחירות, "ארבע מערכות בחירות הוכיחו את מוכנות הוועדה ויכולתה להתמודד בהצלחה עם הגנת סייבר". עוד טענה הוועדה, שחלק גדול מהליקויים שעליהם הצביע המבקר תוקנו עוד ב-2020. "ועדת הבחירות סבורה כי שיח בונה, מקצועי וראוי בנושא הגנת הסייבר הוא שיח רגיש במיוחד, וכל גורם העוסק בתחום בוודאי יסכים כי ראוי לו כי יתנהל בפורומים המקצועיים המתאימים ולא בכיכר העיר, תוך עידוד כל תוקף פוטנציאלי".

מעריב

"לא ניתן להגן הרמטית על הכל": האזהרה לאחר הפריצה למערכות האזעקה

זירת הלחימה בתחום הסייבר הולכת ומתחממת, כאשר מיליוני בני אדם הושפעו מהם ברחבי העולם, בין אם מדובר במידע רפואי מוצפן ובין אם בתחנת דלק שהושבתה. אז מי עומד מאחורי הקרבות?

סתיו נמר

מי שפתח בשנה וחצי האחרונות את מהדורות החדשות בטלוויזיה, או הביט בעמודים הראשונים של העיתונים, נתקל בדיווחים רבים על מתקפות סייבר שהתרחשו בארץ ומחוצה לה. מבלי להתייחס לזהות הקורבנות, המעורבים (והמעורבים לכאורה), קשה לפספס את העובדה שהמתקפות הללו פוגעות ומשפיעות על כלל תחומי החיים ברחבי העולם.

לקראת אירועי שבוע הסייבר שיחלו בשבוע הבא, בהובלת מרכז הסייבר של אוניברסיטת תל אביב בשיתוף מערך הסייבר הלאומי, משרד הכלכלה ומשרד החוץ, וברקע הפריצה למערכות האזעקה בירושלים ובאילת, ישבתי לשיחה מיוחדת עם ד"ר יניב הראל, ראש תחום אסטרטגיה (CSO) במרכז הסייבר של אוניברסיטת תל-אביב. בראשית השיחה, שוחחנו על הגורמים העומדים מאחורי המתקפה - בין אם הם לוקחים על כך אחריות בצורה ישירה ובין אם לאו. "קיים הבדל פעולה מהותי בין גורמי פשיעת סייבר בעולם לבין גורמים מדינתיים", הסביר ד"ר הראל, "גורמי פשיעת סייבר ממוקדים בדרך כלל ביכולת להביא תשלום מהגורם נתקף, ועל כן יעשו את רב מאמציהם כדי למקסם את התשלום הזה. התוקפים ינסו לברר שהגורם הנתקף מסוגל לשלם, ויעשו מה שניתן כדי לגבות ממנו סכום מקסימלי". לדבריו, לגורמי פשיעת הסייבר אין שום טעם להשקיע בחברה או ארגון שידוע מראש שלא יוכל לשלם להם - כי אז ברור שהמאמץ מיותר.

הוא המשיך והסביר כי "גורמים מדינתיים יפעלו דרך כלל בצורה דומה, אולם סוג היעדים שלהם יהיו אחרים. הם לא יפעלו להשגת תשלומי כסף (אם כי יש טענה שמדינות מסוימות משתמשות בערוץ הסייבר גם למטרות כאלו) אלא להשגת אפקטים אסטרטגיים שישרתו את האינטרסים של המדינה אליה שייכים". ד"ר הראל, לשעבר מנכ"ל קבוצת הסייבר של DELL ובכיר במערכת הביטחון, ציין: "פעמים רבות, בחסות היכולת להסתתר, מדינות בוחרות את המדיום הסייברי כדי לפעול בו ולגרום נזק לאחרות או להעביר מסר של אי שביעות רצון ממצבים מסוימים וכו>". הראל מציין כי נכון להיום התחום עדיין לא נמצא בשימוש פעיל על ידי מדינות רבות אולם צפוי שהשימוש רק יגבר. עד כמה הפריצה למערכות האזעקה והפעלתן היא אירוע משמעותי?

"מדינת ישראל, כמו אחרות בעולם, עומדת בפני תקיפות סייבר מסוגים שונים. מן הסתם, תוקפים עשויים לנסות ולפגוע במערכות מרכזיות שונות, ובמידה והם לא מצליחים לעשות זאת - הם עשויים לעבור למערכות אחרות, כדי לרשום הישגים מקומיים כלשהם. בסופו של דבר, אין נזק גדול באופן כללי בפריצה למערכות אזעקה, הן משבשות את החיים למספר דקות ומנסות לפגוע ברוח האזרחים, תוך השפעה על ביטחונם הכללי. אזעקה מקומית עושה זאת לאוכלוסייה ספציפית מאוד. כמובן שלא צריך לזלזל גם בזה, ועלינו לנסות ולמנוע כל סוג תקיפה, אולם חלק מהחוסן הכללי הוא גם לא להתרגש מדברים כאלה, כי לא ניתן להגן הרמטית על הכל, ונכון לשים את רב תשומת הלב לדברים שעלול להיות להם נזק מהותי".

"למרבה ההפתעה, ההיערכות לאירועי סייבר דומה מאוד לתחומים אחרים בהרבה היבטים", הסביר המומחה, "בניגוד לתחומים קונבנציונליים בהם ההערכות לאיום צבאי ולאיום אזרחי נראים אחרת לגמרי, בתחום הסייבר הרבה מהפעולות דומות. עלינו להיות ערניים למערכותינו, לראות שהן מותאמות לצורך ומטופלות כמו כל פלטפורמה אחרת, יש להשקיע במערכות הגנה ובצוותי הגנת סייבר מיומנים בארגונים שלנו, אנחנו צריכים לוודא שיש לנו מתודולוגיות נכונות ושאנחנו נותנים תשומת לב להערכות ולאימונים רלוונטיים כדי שלצוותים תהיה כשירות מבצעית. עלינו לתדרך את העובדים ולייצר מודעות יותר גבוהה לאיומי הסייבר ויש להשקיע גם בחשיבה והערכות למקרה של תקיפות סייבר".

בעצם, עלינו להיערך לתרחיש של מתקפת סייבר ממשית.

"כן, אנחנו רואים הבדל מהותי בין ארגונים שנערכו קודם לבין כאלה שהדבר נופל עליהם בפעם הראשונה, ואני מתכוון לכל הדרגים. לאחרונה, באירוע של תרגול הנהלה בכירה באחת המדינות בה הייתי מעורב, תוך כדי שההנהלה גיבשה המלצה שצריך לעצור סוג של מתקפה ורצוי לשלם כופר כדי לצמצם את הנזק, הפתיע המנכ"ל את שאר חברי ההנהלה והסביר להם שלדעתו לא צריכה להיות בעיה להסביר לציבור את התקיפה והם ייקחו את הסיכון ולא ישלמו. כמובן שהתפתח דיון נרחב בהנהלה על העניין. זו דוגמא מובהקת של התלבטות, שכאשר נעשית בנחת (יחסית), ותוך כדי תרגיל התנאים לבחינת השיקולים השונים, טובה הרבה יותר מבעת מצב אמיתי. יותר מכך, מתפתחת יכולת תקשורת בין הגורמים השונים בארגון שמאפשרת התלבטות משותפת בדברים האלה. ארגונים כאלה מגיעים מוכנים הרבה יותר למצבי אמת".

סוגייה נוספת שעלתה במהלך השיחה היא שאלת המחיר הכלכלי - תג המחיר שמציבים התוקפים בפני הקורבנות. כאמור, ממבט על המקרים שהתרחשו בשנים האחרונות, ניתן לראות כי הסכומים שדווח כי הקורבנות נדרשו לשלם, היה שונה ממדינה למדינה ומיעד תקיפה אחד לאחר. "אין מחיר אחיד, וגם לא בדיוק מחירון, שכן הדרישות של התוקפים משקפות בדרך כלל את מה שצפוי שהארגון יהיה מוכן לשלם על פי רב בקורלציה לגודל של הארגון, סוג הביזנס שלו, גודל ההישגים שהתוקפים חושבים שהשיגו במסגרת התקיפה, ורוח התקופה שגם היא משתנה מעת לעת", הסביר.

לדבריו, את המחיר הזה יש לחבר לסיכוי לקבל את הכסף. "כאן נכנסת אבחנה חשובה לגבי השיטה: בשונה מכל התקשרות בין שני גורמים, בהם בדרך כלל ניתנת הצעה לפני, מסכימים על מחיר ואז מתבצעת העבודה או השירות - בתחום מתקפות הכופר סדר העניינים הוא הפוך. קודם התוקף עושה את כל העבודה, מנסה לתקוף, לחדור לארגון, להשיג נכסים בעלי משמעות ועוד, ורק אז הוא פונה ללקוח ומנסה לגבות כסף", ציין ד"ר יניב הראל, "מסיבה זו, כאשר מתקיים ניסיון הגבייה, התוקף כבר השקיע את מאמציו, וכעת יש שאלה כמה יצליח לגבות על ההישגים שהשיג. בשלב הזה מתקיים קרב מוחות בין התוקף שמנסה למקסם את הסכום ובכלל להבין אם יקבל כסף, לבין הנתקף שמעדיף לא לשלם ואם כן אז כמה שפחות."בשנה האחרונה ראינו תוקפים שהפסיקו את מאמצי התקיפה כעבור מספר ימים, לאחר שהעריכו כי לא יצליחו להשיג תשלום, או כאלה שלא התמידו במשא ומתן - גם כן מסיבה זו", אמר.

נשמע שרמת המומחיות של התוקף היא צד רלוונטי נוסף.

"בהחלט. מדובר במשא ומתן בין תוקפים שעושים זאת מדי שבוע, לעומת חברות שחושבות שיעשו זאת עם שכל ישר והיגיון בריא, אך הן מגלות את חשיבות המומחיות דרך ההתנסות השלילית. באופן כללי, בתחום הסייבר קמים תחומי התמחות חשובים וחדשים, ונבנית תורה בתחומים שונים בתקופה זו של העולם".

ISRAELDEFENSE

ראש מערך הסייבר הלאומי: "אנחנו רואים את האיראנים במרחב הסייבר"

בהתייחס לסוגי התוקפים אמר, "מגוון התוקפים בזירת הסייבר הורחב וכולל גם תוקפים נוספים, קבוצות תקיפה, שלוחות של מדינות, ארגוני פשיעה, אנשים פרטיים ועוד"

עמי רוחקס דומבה

בנאום ראשון מאז כניסתו לתפקיד לפני כארבעה חודשים, הציג גבי פורטנוי, ראש מערך הסייבר הלאומי את הפרויקט החדש של המערך ליצירת כיפת סייבר על המרחב האזרחי.

בהתייחס לתוקפים במרחב אמר פורטנוי כי: "איראן הפכה לשחקן מרכזי שאנו מזהים במרחב הסייבר, יחד עם חמאס וחיזבאללה. אנחנו רואים אותם, אנחנו יודעים איך הם עובדים ואנחנו שם". את הדברים הציג פורטנוי בכנס כחלק משבוע הסייבר, שמתקיים השבוע בהובלת מערך הסייבר הלאומי והמרכז למחקר סייבר באוניברסיטת תל אביב.

על פי נתוני מערך הסייבר הלאומי שהוצגו בכנס, בשנה האחרונה בלם המערך כ-1,500 נסיונות תקיפה שונים על העורף הישראלי. לדברי פורטנוי בכנס, "למערך יש נקודת תצפית ייחודית על ההגנה המדינתית. אנחנו עוברים להסתכלות מגזרית על המשק – הסתכלות על פי תחומים ולא על פי גופים. אנחנו עוברים מפרדיגמה שמסתכלת על התוקף לפרדיגמה שמסתכלת על העורף האזרחי".

בהתייחס לסוגי התוקפים אמר, "מגוון התוקפים בזירת הסייבר הורחב וכולל גם תוקפים נוספים, קבוצות תקיפה, שלוחות של מדינות, ארגוני פשיעה, אנשים פרטיים ועוד".

בהמשך דבריו הציג פורטנוי את הפתרון החדש שמקדם המערך להגנה על המשק: "אנחנו צריכים כיפת ברזל הגנתית בתחום הסייבר לטובת אזרחי מדינת ישראל. כיפת הסייבר היא פרויקט הדגל החדש שלנו במערך לחיזוק הגנת הסייבר של המשק כולו.

"הפרויקט יעשה שימוש במנגנונים חדשים ויביא לצמצום מתקפות הסייבר בצורה משמעותית. כיפת הסייבר היא גישה פרו-אקטיבית חדשה לחיזוי ובלימת מתקפות שמשלבת טכנולוגיות של ביג-דאטא ובינה מלאכותית".

פורטנוי הציג את ההרחבה של הכלים של המערך ופתיחתם מהטמעה בתשתיות הקריטיות בלבד לסקטורים ותחומים נוספים. לסיכום אמר כי "רק באמצעות שיתוף פעולה – בין מדינות, עם חברות הגנת הסייבר, האקדמיה, הממשל וגופי הבטחון - נוכל להגן על עצמנו במלחמת הסייבר וליצור כיפת ברזל הגנתית בסייבר רחבה".

ערוץ 7 www.inn.co.il

ראש מערך הסייבר: "איראן שחקן מרכזי שאנחנו מזהים במרחב, מקדמים כיפת סייבר"

בנאום מקיף ראשון מאז כניסתו לתפקיד לפני כארבעה חודשים, הציג היום גבי פורטנוי, ראש מערך הסייבר הלאומי את הפרויקט החדש של המערך ליצירת כיפת סייבר על המרחב האזרחי. בשנה האחרונה בלם המערך כ-1,500 ניסיונות תקיפה שונים על העורף הישראלי.

בהתייחס לתוקפים במרחב אמר פורטנוי כי: "איראן הפכה לשחקן מרכזי שאנו מזהים במרחב הסייבר, יחד עם חמאס וחיזבאללה. אנחנו רואים אותם, אנחנו יודעים איך הם עובדים ואנחנו שם". את הדברים הציג פורטנוי בכנס כחלק משבוע הסייבר, שמתקיים השבוע בהובלת מערך הסייבר הלאומי והמרכז למחקר סייבר באוניברסיטת תל אביב.

ערוץ 7 www.inn.co.il

ראש מערך הסייבר: איראן הפכה לשחקן מרכזי שאנו מזהים במרחב הסייבר

איראן הפכה לשחקן מרכזי שאנו מזהים במרחב הסייבר, יחד עם חמאס וחיזבאללה

ניצן קידר

בנאום מקיף ראשון מאז כניסתו לתפקיד לפני כארבעה חודשים, הציג היום (ג') גבי פורטנוי, ראש מערך הסייבר הלאומי את הפרויקט החדש של המערך ליצירת כיפת סייבר על המרחב האזרחי.

בהתייחס לתוקפים במרחב אמר פורטנוי כי "איראן הפכה לשחקן מרכזי שאנו מזהים במרחב הסייבר, יחד עם חמאס וחיזבאללה. אנחנו רואים אותם, אנחנו יודעים איך הם עובדים ואנחנו שם".

את הדברים הציג פורטנוי בכנס שבוע הסייבר שמתקיים באוניברסיטת תל אביב. לדברי פורטנוי בכנס, "למערך יש נקודת תצפית ייחודית על ההגנה המדינתית. אנחנו עוברים להסתכלות מגזרית על המשק – הסתכלות על פי תחומים ולא על פי גופים. אנחנו עוברים מפרדיגמה שמסתכלת על התוקף לפרדיגמה שמסתכלת על העורף האזרחי".

בהתייחס לסוגי התוקפים אמר, "מגוון התוקפים בזירת הסייבר הורחב וכולל גם תוקפים נוספים, קבוצות תקיפה, שלוחות של מדינות, ארגוני פשיעה, אנשים פרטיים ועוד".

בהמשך דבריו הציג פורטנוי את הפתרון החדש שמקדם המערך להגנה על המשק: "אנחנו צריכים כיפת ברזל הגנתית בתחום הסייבר לטובת אזרחי מדינת ישראל. כיפת הסייבר היא פרויקט הדגל החדש שלנו במערך לחיזוק הגנת הסייבר של המשק כולו. הפרויקט יעשה שימוש במנגנונים חדשים ויביא לצמצום מתקפות הסייבר בצורה משמעותית. כיפת הסייבר היא גישה פרו-אקטיבית חדשה לחיזוי ובלימת מתקפות שמשלבת טכנולוגיות של ביג-דאטא ובינה מלאכותית".

פורטנוי הציג את ההרחבה של הכלים של המערך ופתיחתם מהטמעה בתשתיות הקריטיות בלבד לסקטורים ותחומים נוספים. לסיכום אמר כי "רק באמצעות שיתוף פעולה – בין מדינות, עם חברות הגנת הסייבר, האקדמיה, הממשל וגופי הבטחון - נוכל להגן על עצמנו במלחמת הסייבר וליצור כיפת ברזל הגנתית בסייבר רחבה".

ynet ידיעות אחרונות

סגן יחידת 8200: "אנו יודעים שלגיוסים שלנו יש השפעה על הגיוון בהייטק הישראלי"

אורי, סגן מפקד יחידת 8200, אמר בכנס הסייבר השנתי שנערך באוניברסיטת תל אביב כי "יש לנו אחריות כלפי החברה הישראלית. אנחנו יודעים שלגיוון בגיוסים שלנו יש השפעה אחר כך על הגיוון בהייטק הישראלי". לדבריו, "לצד יחידות נוספות בצה"ל, הרחבנו בשנה שעברה את תוכנית <גשרים> מתיכונים לחטיבות הביניים, ובשנה הבאה נרחיב את התוכנית ליותר מ-20 רשויות נוספות". הוא הוסיף: "אנחנו צופים השתתפות של יותר מ-20 אלף בני נוער. בעשור האחרון קלטנו צעירים רבים גם מהפריפריה, ואני בטוח שזה ישפיע על התעשייה והחברה גם בעשור הקרוב".

בנט מאיים: "אם תתעסקו עם ישראל - תשלמו מחיר"

ראש הממשלה נאם בכנס הסייבר באוניברסיטת תל אביב והצהיר כי "אי אפשר לפגוע בישראל דרך צד שלישי ולהתחמק מזה. אם מישהו יתקוף אותנו בסייבר - אנחנו נתקוף בחזרה"

יאיר מור

ראש הממשלה, נפתלי בנט, דיבר לפני זמן קצר בכנס שבוע הסייבר שנפתח היום באוניברסיטת תל אביב, והצהיר כי ישראל מסוגלת להתמודד עם כל האיומים הקיימים בתחום.

"בצד ההגנתי, אני לא רוצה להגיד שהכל מושלם", הודה בנט, והמשיך: "אבל סך הכל מצבנו די טוב; אי אפשר יותר לפגוע בישראל דרך צד שלישי ולהתחמק מזה. כמו שיש הרתעה גרעינית – תהיה גם הרתעה בסייבר. הגישה שלי לאויבינו – במיוחד לאיראן – היא שלא נמיט הרס, אבל אם תתעסקו עם ישראל – תשלמו מחיר. אם הבריון שולח אנשים להכות אותנו – אנחנו הולכים להכות את הבריון בכל הממדים. אם מישהו יתקוף אותנו בסייבר – אנחנו נתקוף בחזרה", הבהיר בנט.

לדבריו, תחום לוחמת הסייבר ממש מחליף את הלוחמה הרגילה. "היום אתה יכול לעשות דברים לפגוע באויב שלך באמצעות סייבר שבעבר היה דורש 50-100 לוחמים מאחורי קווי האויב, עם סיכון עצום. עכשיו, חבורה של אנשים חכמים שיושבים ליד מקלדת יכולים להשיג את אותו הדבר". לכן, הוא אומר, "באופן בלתי נמנע, הסייבר הולך להפוך לאחד הממדים הבולטים ביותר של לוחמה עתידית". הוא אף הודה כי "קצת הופתעתי מהמחסור בכלי סייבר במלחמה באוקראינה – חשבתי שזה יהיה הרבה יותר מתקדם והרבה יותר מסיבי".

מעבר לפן המדיני של הסייבר, דיבר בנט גם עם הפן העסקי שלו. "תאגידים צריכים לקחת אחריות משלהם, וכשהם מתעסקים בנתוני הלקוחות שלהם – זו הבעיה שלהם. אבל זה לא מספיק – ברמה הלאומית, מערך הסייבר, בראשות (תא"ל במיל> גבי) פורטנוי, עובד עם החברות כדי לעזור להן להגן על עצמן, עם התשתיות הקריטיות".

ראש הממשלה נגע גם בשילוב קהילות שונות בתעשיית ההייטק בכלל והסייבר בפרט. "אני רואה ארבעה מקורות שונים של כישרונות חדשים בהייטק ובסייבר: הקבוצה הראשונה היא החרדים – הם לא חלק משמעותי מהמשק, למרות יכולותיהם. הגישה שלי לא הייתה פופולארית, ועכשיו זו מדיניות. אנחנו צריכים לתת להם פטור משירות בצבא ולתת להם להצטרף לכוח העבודה במקום להכריח אותם להישאר בישיבות. זה מאתגר, כי הם פחות מיומנים באנגלית. אולי זה לא הדבר הצודק, אבל זה הדבר הנכון; הקבוצה השנייה היא נשים מהחברה הערבית. תחום ההייטק צריך להיות פתוח להבאת אנשים שונים, במיוחד מהפריפריה. במשך שנים רבות הפריפריה לא זכתה לשירות וזו פשוט הייתה מדיניות לא נכונה של ישראל. ולבסוף, נתתי את האישור להצטרפות מיידית של עובדים פלסטינים להייטק הישראלי, כולל אישורי תנועה לבוא לכאן".

גנץ: "איראן מנסה להתערב בתהליכים דמוקרטים בישראל"

בכנס הסייבר שנערך באוניברסיטת תל אביב שר הביטחון למלחמת הסייבר בין איראן לישראל וחשף פרטים חדשים אודות המאבק החדש

שר הביטחון בני גנץ התארח הבוקר (רביעי) בכנס הסייבר הבינלאומי של מרכז הסייבר באוניברסיטת ת"א. במסגרת הכנס שר הביטחון נשא נאום ואמר: "ישראל מכירה את מערכות הסייבר של יריביה ואת דרכי הפעולה שלהם. אנו רואים בשנים האחרונות תופעה של קבוצות האקרים מטעם איראן, שפועלות מול ישראל ומדינות נוספות. <השלוחים החדשים>, הם טרוריסטים עם מקלדת שדינם כמו לוחמי ארגוני טרור אחרים."

גנץ הוסיף ואמר " אנחנו יודעים מי הם, אנחנו פוגעים בהם ובשולחיהם, וגם היום הם על הכוונת שלנו – ולא רק במימד הקיברנטי. שום מתקפה מול אזרחי ישראל לא תעבור לסדר היום. והאחריות היא של התוקפים ושל המדינה שממממנת ושולחת אותם. תקיפת סייבר יכולה להיענות במגוון דרכים במרחב הסייבר ובמרחבים נוספים".

כמו כן שר הביטחון התייחס לזירת המלחמה המודרנית שמשתנה בשנים האחרונות ואמר: "בשנים הקרובות נצטרך גם לבחון את צורת ההתארגנות, הניהול והתפעול של לוחמת הסייבר, על מאפייניה ההתקפיים וההגנתיים בצה"ל ובמערכת הביטחון כולה"

בנוסף לכך גנץ חשף נתונים מפתיעים על פעילות מערך הסייבר האיראני ותיאר כי למשרד הביטחון יש את המידע על כך שהיה ניסיון איראני להתערב במערכת הבחירות בארה"ב ובישראל. יתרה מזו, גנץ תיאר כי כפי שנחשף במחקרים ההאקרים האיריים מנסים ללא הפסקה ובכול הכוח לפגוע בספינות, תחנות דלק ומפעלי תעשייה במספר מדינות.

ערוץ 7
www.inn.co.il

בני גנץ חושף: איראן ניסתה לפגוע בכוח יוניפי"ל בלבנון

שר הביטחון התייחס בכנס הסייבר גם לסרטון שפרסם חמאס: "ניסיונות סחטנות ותרגילי תודעה לא ישפיעו על התנהלותנו".

שר הביטחון בני גנץ נשא דברים הבוקר (רביעי) בנאום במסגרת כנס הסייבר הבינלאומי של מרכז הסייבר באוניברסיטת ת"א.

גנץ התייחס בדבריו לסרטון של השבוי הישאם א-סייד שפרסם חמאס ואמר: "אתמול פורסם סרטון שמטרתו סחטנות – על גבה של סוגייה הומניטארית. חמאס מחזיק בשבי את ארבעת הבנים בניגוד לחוק הבינלאומי, בניגוד למוסר. חמאס אחראית לכך והציפייה שלנו מהקהילה הבינלאומית היא לפעול מול ההתנהלות הנפשעת הזו של חמאס".

"מדינת ישראל פועלת במגוון אמצעים, וממשיכה להפוך כל אבן על מנת להשיב את הבנים הביתה. כפי שאמרנו בעבר – מדובר בסוגיה הומניטארית, כך אנו רואים אותה, ועל הבסיס הזה נמשיך לפעול. ניסיונות סחטנות ותרגילי תודעה לא ישפיעו על עמדתנו והתנהלותנו", דברי גנץ.

הוא חשף כי איראן מנסה לפגוע בכוחות בינלאומיים המוצבים בלבנון. "איראן מפעילה את שלוחיה גם במימד הסייבר: אני יכול לחשוף היום, שלאחרונה אותרה פעילות של גופי הביטחון האיראנים בשיתוף עם חיזבאללה, בכדי לפגוע בפעילות כוחות יוניפי"ל בלבנון. זאת על ידי מימוש מבצע בסייבר שמטרתו הייתה לגנוב חומרים על היערכות יוניפ"ל במרחב, ושימוש בהם על ידי חיזבאללה. זוהי פגיעה נוספת של איראן וחיזבאללה באזרחי לבנון, וביציבותה של לבנון".

לדבריו, "ישראל מכירה את מערכות הסייבר של יריביה ואת דרכי הפעולה שלהם. אנו רואים בשנים האחרונות תופעה של קבוצות האקרים מטעם איראן, שפועלות מול ישראל ומדינות נוספות. "השלוחים החדשים", הם טרוריסטים עם מקלדת שדינם כמו לוחמי ארגוני טרור אחרים. אנחנו יודעים מי הם, אנחנו פוגעים בהם ובשולחיהם, וגם היום הם על הכוונת שלנו – ולא רק במימד הקיברנטי. שום מתקפה מול אזרחי ישראל לא תעבור לסדר היום. והאחריות היא של התוקפים ושל המדינה שממנת ושולחת אותם. תקיפת סייבר יכולה להיענות במגוון דרכים במרחב הסייבר ובמרחבים נוספים."

עוד אמר כי "איראן מובילה את טרור הסייבר – ועושה מהלכים שמטרתם להשפיע על תהליכים דמוקרטיים ועל ממשלים, כפי שקרה בבחירות לנשיאות ארצות הברית ובניסיונות נוספים שישראל מודעת אליהם. פעולות כמו זו של יחידת "שאהיד כאווה" שאספה מידע על ספינות, תחנות דלק ומפעלי תעשייה במספר מדינות, נעשו תחת דירקטיבה ישירה של ההנהגה האיראנית ומשמרות המהפכה כפי שנחשף בתחקירים."

שר הביטחון ציין כי "בשנים האחרונות בלמנו ניסיונות רבים לפרוץ לחברות פרטיות וציבוריות, בארץ ובחו"ל. אני קורא גם לציבור לדרוש "אחריות קיברנטית", ולהעניש חברות וגופים שלא פועלים בהתאם להנחיות."

A"המשימה העליונה שלנו, בצבא, בתעשיות ובארגוני הביטחון השונים היא לבנות את האנשים, להכשיר אותם, ולהשאיר אותם. אני והרמטכ"ל הצבנו את הנושא הזה כאחת המשימות המרכזיות ביחידות הרלבנטיות. אנחנו בוחנים את בניין הכוח כל העת – גם בהיקפי כוח האדם, גם בנושא ההכשרות וגם בנושא המשימות. בשנים הקרובות נצטרך גם לבחון את צורת ההתארגנות, הניהול והתפעול של לוחמת הסייבר, על מאפייניה ההתקפיים וההגנתיים בצה"ל ובמערכת הביטחון כולה. יש חשיבות גדולה לשיתופי הפעולה שלנו עם העולם מול איראן גם במימד הסייבר. את אותם שיתופי פעולה שאנו בונים באזור מול איראן בהיבטים של הגנה מול איומים שונים – אנחנו מרחיבים גם במימד הסייבר", סיכם.

טלנירי
מידע פיננסי לפני כולם

המבקר אנגלמן בשבוע הסייבר הבינלאומי של אוניברסיטת תל אביב: "מלחמת העולם השלישית תהיה מלחמת סייבר אך העולם לא ערוך אליה"

מבקר המדינה מתניהו אנגלמן השתתף היום בשבוע הסייבר השנתי של אוניברסיטת תל אביב ונתן סקירה מקיפה, לראשונה, על ביקורת הסייבר אותה הוא מבצע החל מכניסתו לתפקיד – אז הקים אגף סייבר מיוחד.

"הסייבר היום חשוב מתמיד", פתח אנגלמן. "במובן מסוים, כולנו חיים בתוך תכנית <האח הגדול> בינלאומית. כמבקר מדינת ישראל וסגן נשיא EUROSAI, אני חייב לחלוק איתכם אמירה פסימית: אנחנו חשופים. לאזרחי העולם אין הגנה. הנתונים שלנו גלויים ליותר מדי אנשים. הכסף שלנו חשוף, הילדים שלנו חשופים, הבריאות שלנו חשופה, הביטחון שלנו חשוף. מלחמת העולם השלישית תהיה מלחמת סייבר, אבל העולם לא מוכן אליה.

עם כניסתי לתפקיד הנוכחי של מבקר המדינה, ולנוכח איומי הסייבר ההולכים וגדלים איתם מתמודדת מדינת ישראל בשנים האחרונות, החלטתי להציב את תחום הסייבר כאחד מבעיות הליבה בהן תעסוק הביקורת. הוקמו חטיבת ביקורת סייבר וחטיבה ייעודית לביקורת מערכות מידע. בהתחלה היו כאלה ש>הרימו גבה<. היום אין מי שלא מבין את חשיבות הנושא. גם ארגון המבקרים הבינלאומי קבע כי הגנה כזו על מערכות מידע היא אחד הסיכונים הגדולים ביותר".

אנגלמן סיפר כי במסגרת ביקורות הסייבר הוא בודק את הגנת הפרטיות, מנגנוני בקרה והגנה של המערכות הממוחשבות; השקעה ב-IT, היערכות מוקדמת לאירועי סייבר והתאוששות מאסון, התקפות סייבר ופגיעה בתשתיות מדינה קריטיות. ועוד. כמו כן, הוא הנחה לקיים מבחני חדירה על ידי חברות האקרים מטעם משרד מבקר המדינה.

"דו"ח על מערכת המחשוב של ועדת הבחירות המרכזית בישראל מצא כי מערכת המחשוב המרכזית שלהם החלה לפעול בשנת 2008 והיא חגגה "בר מצווה" בשנה שעברה. ועדיין, ביקורות סייבר נערכו רק בתקופות בחירות, כך שלא ניתן היה לבצע בדיקות מקיפות ומורכבות שכללו את כל ההיבטים הנדרשים להגנת הסייבר.

בשנה האחרונה ביצענו בדיקות חדירה במרכז ניהול התנועה בירושלים, בבתי חולים ובמערכות רשות המסים. בביקורות מצאנו ליקויים משמעותיים, לרבות העובדה שמעט מאוד בדיקות חדירה בוצעו על ידי גופים ציבוריים וחלקם ערכו בדיקות חדירה רק במהלך הביקורת; אנו במשרד מבקר המדינה מתחייבים להמשיך ולהתייחס לנושא משמעותי זה ביתר שאת, לטובת אזרחי ישראל והעולם כולו".

מדשות מבזק לייב

אנגלמן: אנחנו חשופים, נטולי הגנה, חיים בתוך תכנית עולמית של 'האח הגדול'

"עלו ליקויים משמעותיים במוכנות ועדת הבחירות המרכזית לאיומי הסייבר", אמר מבקר המדינה מתניהו אנגלמן בשבוע הסייבר הבינלאומי של אוניברסיטת תל אביב.

איתמר רובינשטיין

מבקר המדינה מתניהו אנגלמן השתתף היום (רביעי) בכנס הסייבר השנתי של אוניברסיטת תל אביב ונתן סקירה מקיפה, לראשונה, על ביקורת הסייבר אותה הוא מבצע החל מכניסתו לתפקיד – אז הקים אגף סייבר מיוחד.

"הסייבר היום חשוב מתמיד", פתח אנגלמן. "במובן מסוים, כולנו חיים בתוך תכנית <האח הגדול> בינלאומית. כמבקר מדינת ישראל וסגן נשיא EUROSAI, אני חייב לחלוק איתכם אמירה פסימית: אנחנו חשופים. לאזרחי העולם אין הגנה. הנתונים שלנו גלויים ליותר מדי אנשים. הכסף שלנו חשוף, הילדים שלנו חשופים, הבריאות שלנו חשופה, הביטחון שלנו חשוף. מלחמת העולם השלישית תהיה מלחמת סייבר, אבל העולם לא מוכן אליה.

עם כניסתי לתפקיד הנוכחי של מבקר המדינה, ולנוכח איומי הסייבר ההולכים וגדלים איתם מתמודדת מדינת ישראל בשנים האחרונות, החלטתי להציב את תחום הסייבר כאחד מבעיות הליבה בהן תעסוק הביקורת. הוקמו חטיבת ביקורת סייבר וחטיבה ייעודית לביקורת מערכות מידע. בהתחלה היו כאלה ש>הרימו גבה<. היום אין מי שלא מבין את חשיבות הנושא. גם ארגון המבקרים הבינלאומי קבע כי הגנה כזו על מערכות מידע היא אחד הסיכונים הגדולים ביותר". אנגלמן סיפר כי במסגרת ביקורות הסייבר הוא בודק את הגנת הפרטיות, מנגנוני בקרה והגנה של המערכות הממוחשבות; השקעה ב-IT, היערכות מוקדמת לאירועי סייבר והתאוששות מאסון, התקפות סייבר ופגיעה בתשתיות מדינה קריטיות. ועוד. כמו כן, הוא הנחה לקיים מבחני חדירה על ידי חברות האקרים מטעם משרד מבקר המדינה.

לדבריו, "דו"ח על מערכת המחשוב של ועדת הבחירות המרכזית בישראל מצא כי מערכת המחשוב המרכזית שלהם החלה לפעול בשנת 2008 והיא חגגה "בר מצווה" בשנה שעברה. ועדיין, ביקורות סייבר נערכו רק בתקופות בחירות, כך שלא ניתן היה לבצע בדיקות מקיפות ומורכבות שכללו את כל ההיבטים הנדרשים להגנת הסייבר.

בשנה האחרונה ביצענו בדיקות חדירה במרכז ניהול התנועה בירושלים, בבתי חולים ובמערכות רשות המסים. בביקורות מצאנו ליקויים משמעותיים, לרבות העובדה שמעט מאוד בדיקות חדירה בוצעו על ידי גופים ציבוריים וחלקם ערכו בדיקות חדירה רק במהלך הביקורת; אנו במשרד מבקר המדינה מתחייבים להמשיך ולהתייחס לנושא משמעותי זה ביתר שאת, לטובת אזרחי ישראל והעולם כולו".

מדשות מבזק לייב

ראש מערך הסייבר הלאומי: "איראן הפכה לשחקן מרכזי"

בנאום מקיף ראשון מאז כניסתו לתפקיד לפני כארבעה חודשים, הציג היום (שלישי) גבי פורטנוי, ראש מערך הסייבר הלאומי את הפרויקט החדש של המערך ליצירת כיפת סייבר על המרחב האזרחי. בהתייחס לתוקפים במרחב אמר פורטנוי כי: "איראן הפכה לשחקן מרכזי שאנו מזהים במרחב הסייבר, יחד עם חמאס וחיזבאללה. אנחנו רואים אותם, אנחנו יודעים איך הם עובדים ואנחנו שם".

את הדברים הציג פורטנוי בכנס שבוע הסייבר, שמתקיים השבוע בהובלת מערך הסייבר הלאומי והמרכז למחקר סייבר באוניברסיטת תל אביב.

על פי נתוני מערך הסייבר הלאומי שהוצגו בכנס, בשנה האחרונה בלם המערך כ-1,500 נסיונות תקיפה שונים על העורף הישראלי. לדברי פורטנוי בכנס, "למערך יש נקודת תצפית ייחודית על ההגנה המדינתית. אנחנו עוברים להסתכלות מגזרית על המשק – הסתכלות על פי תחומים ולא על פי גופים. אנחנו עוברים מפרדיגמה שמסתכלת על התוקף לפרדיגמה שמסתכלת על העורף האזרחי".

בהתייחס לסוגי התוקפים אמר, "מגוון התוקפים בזירת הסייבר הורחב וכולל גם תוקפים נוספים, קבוצות תקיפה, שלוחות של מדינות, ארגוני פשיעה, אנשים פרטיים ועוד".

בהמשך דבריו הציג פורטנוי את הפתרון החדש שמקדם המערך להגנה על המשק: "אנחנו צריכים כיפת ברזל הגנתית בתחום הסייבר לטובת אזרחי מדינת ישראל. כיפת הסייבר היא פרויקט הדגל החדש שלנו במערך לחיזוק הגנת הסייבר של המשק כולו. הפרויקט יעשה שימוש במנגנונים חדשים ויביא לצמצום מתקפות הסייבר בצורה משמעותית. כיפת הסייבר היא גישה פרו-אקטיבית חדשה לחיזוי ובלימת מתקפות שמשלבת טכנולוגיות של ביג-דאטא ובינה מלאכותית".

פורטנוי הציג את ההרחבה של הכלים של המערך ופתיחתם מהטמעה בתשתיות הקריטיות בלבד לסקטורים ותחומים נוספים. לסיכום אמר כי "רק באמצעות שיתוף פעולה – בין מדינות, עם חברות הגנת הסייבר, האקדמיה, הממשל וגופי הבטחון – נוכל להגן על עצמנו במלחמת הסייבר וליצור כיפת ברזל הגנתית בסייבר רחבה".

מדשות מבזק לייב

1500 ניסיונות תקיפה: ראש מערך הסייבר הלאומי בסקירה

ראש מערך הסייבר חושף כי מתחילת השנה נבלמו 1,500 ניסיונות תקיפה של העורף | לדבריו, איראן היא שחקנית מרכזית במרחב הסייבר, לצד חמאס וחיזבאללה: "צריכים כיפת ברזל הגנתית בתחום הסייבר שיהווה פרויקט דגל חדש"

יוסי ריינר

כ- 1500 ניסיונות של תקיפת סייבר בעורף הישראלי נבלמו מתחילת השנה, כך אמר היום (שלישי) ראש המערך הסייבר הלאומי גבי פורטנוי בנאום בכנס הסייבר הבינלאומי באוניברסיטת תל אביב.

לדבריו, "איראן הפכה לשחקן מרכזי שאנו מזהים במרחב הסייבר, יחד עם חמאס וחיזבאללה. אנחנו רואים אותם, אנחנו יודעים איך הם עובדים ואנחנו שם". אמר פורטנוי.

כאמור, על פי נתוני מערך הסייבר הלאומי שהוצגו בכנס, בשנה האחרונה בלם המערך כ-1,500 נסיונות תקיפה שונים על העורף הישראלי.

עוד הוסיף פורטנוי בכנס, "למערך יש נקודת תצפית ייחודית על ההגנה המדינתית. אנחנו עוברים להסתכלות מגזרית על המשק – הסתכלות על פי תחומים ולא על פי גופים. אנחנו עוברים מפרדיגמה שמסתכלת על התוקף לפרדיגמה שמסתכלת על העורף האזרחי".

בהתייחס לסוגי התוקפים אמר, "מגוון התוקפים בזירת הסייבר הורחב וכולל גם תוקפים נוספים, קבוצות תקיפה, שלוחות של מדינות, ארגוני פשיעה, אנשים פרטיים ועוד".

בהמשך דבריו הציג פורטנוי את הפתרון החדש שמקדם המערך להגנה על המשק: "אנחנו צריכים כיפת ברזל הגנתית בתחום הסייבר לטובת אזרחי מדינת ישראל. כיפת הסייבר היא פרויקט הדגל החדש שלנו במערך לחיזוק הגנת הסייבר של המשק כולו. הפרויקט יעשה שימוש במנגנונים חדשים ויביא לצמצום מתקפות הסייבר בצורה משמעותית. כיפת הסייבר היא גישה פרו-אקטיבית חדשה לחיזוי ובלימת מתקפות שמשלבת טכנולוגיות של ביג-דאטא ובינה מלאכותית".

פורטנוי הציג את ההרחבה של הכלים של המערך ופתיחתם מהטמעה בתשתיות הקריטיות בלבד לסקטורים ותחומים נוספים. לסיכום אמר כי "רק באמצעות שיתוף פעולה – בין מדינות, עם חברות הגנת הסייבר, האקדמיה, הממשל וגופי הבטחון - נוכל להגן על עצמנו במלחמת הסייבר וליצור כיפת ברזל הגנתית בסייבר רחבה".

טלנירי
מידע פיננסי לפני כולם

סגן מפקד יחידת 8200 בשבוע הסייבר השנתי באוניברסיטת ת"א

"סיכלנו ניסיונות להשתלט על מערכות המים הקריטיות של ישראל וכן על תוקפים שניסו לפגוע בתחנות הכוח בארה"ב"

אורי, סגן מפקד יחידת 8200 בשבוע הסייבר השנתי בהובלת המרכז למחקר סייבר באוניברסיטת ת"א, מערך הסייבר הלאומי, משרד הכלכלה ומשרד החוץ: "זוהי ההופעה הפומבית הרשמית הראשונה של 8200. . זאת למרות שמזה כבר כמה עשרות שנים אנחנו מהווים חלק ניכר ממערך ההגנה והמודיעין של ישראל והמשימה שלנו היא איסוף מודיעין על איומים מכריעים על ישראל. ידוע לכל שאנחנו מהווים שחקן מרכזי בתחום הסייבר בישראל ומעבדים את המידע באמצעות כלים שפותחו אצלנו. המידע שאנו מקבלים מגיע ממקורות שונים משותפים, ובעיקר *בזכות פעולה אקטיבית במרחב הסייבר אל מול רשתות יעד ותשתיות ארגוני טרור*. אנחנו חיים בסביבה קשה וזה מצריך מאיתנו לעבוד קשה בסביבה דינמית ואינטנסיבית שמספקת אתגרים חדשים מדי יום. כשאנחנו מצליחים אנחנו מצילים חיים. כשאנחנו נכשלים זה הופך לבעיה גדולה עבור האומה שלנו.

מדי שנה אנחנו קולטים בין 1000-2000 מגויסים בגילאי 18, *וזה הופך את הצוות שלנו לצעיר מאוד כאשר 73% מכוח האדם שלנו מתחת לגיל 23.* בנוסף, ערכי הליבה שמנחים אותנו הם ערכי הדמוקרטיה והאתיקה לצד נהלי קבלת החלטות צבאיים תוך מתן אפשרות לאנשים להביע את דעותיהם ודאגותיהם. *השילוב של גורמים אלו הם הכוח שמייחד אותנו בהשוואה לסוכנויות ויחידות דומות אחרות.*

היחידה שלנו היא חלק מרכזי במערך המודיעין וההגנה של ישראל ואנחנו עובדים בשיתוף פעולה עם היחידות האחרות. *סיכול איומי סייבר (CCO - Counter Cyber Operations) הוא חלק מרכזי בפעילות שלנו.* מטרתנו להשיג עליונות על התוקף, להצליח לזהות אותו ולפעול כדי לשלול את יכולותיו. *כך לעיתים אנו גם מוצאים קורבנות מחוץ לישראל ואז אנו יוצרים קשר עם סוכניות אחרות אם צריך*. אנו עושים זאת גם באופן עצמאי וגם על ידי שיתוף פעולה עם התעשייה וסוכנויות אחרות, באמצעות יישום ושימוש בכלים שפיתחנו. 8200 לא תנוח עד שהאיום יוסר.

כך לדוגמה *סיכלנו את הניסיון להשתלט על מערכות המים הקריטיות של ישראל ולהרעיל אותן לפני מספר שנים. במקרה אחר זיהינו גם כי יריב מסוים תקף את ישראל ותוך כדי זיהינו שאותו תוקף ניסה גם לכוון לתחנות כוח בארה"ב.* זו הייתה האינדיקציה הראשונה להתקפה זו. את האיום הזה הצלחנו למנוע באמצעות שיתוף פעולה הדוק עם השותפים האמריקאים שלנו. הישגים כאלו הם שגורמים לחיילים שלנו להיות גאים בעבודתם ב-8200.

דבר נוסף המחייב הדגשה הוא *האחריות שיש לנו כלפי החברה הישראלית ואנחנו יודעים שלגיוון בגיוסים שלנו יש השפעה אחר כך על הגיוון בהייטק הישראלי*. לצד יחידות נוספות בצה"ל הרחבנו בשנה שעברה את תכנית <גשרים> מתיכונים לחטיבות הביניים ובשנה הבאה נרחיב את התכנית ליותר מ-20 רשויות נוספות *ואנחנו צופים השתתפות של יותר מ-20 אלף בני נוער. בעשור האחרון, קלטנו צעירים רבים גם מהפריפריה ואני בטוח שזה ישפיע על התעשייה והחברה גם בעשור הקרוב.*

רוב מה שאנחנו עושים הוא חסוי ואנחנו פועלים על מנת למנוע איומי סייבר נגד ישראל ומבטיחים שישראל תישאר מעצמה מובילה בתחום הטכנולוגיה והסייבר באזורנו. *בתוך המרחה הזה יש לנו אחריות על אתיקה, מוסר וערכים ואנו לוקחים אותה ברצינות רבה, תוך שמירת מחויבות לערכים הדמוקרטיים שלנו, לנורמות במרחב הסייבר, ולחברה הישראלית וזו הסיבה העיקרית שאני עומד פה היום*.

אודות שבוע הסייבר הלאומי השנתי:

שבוע הסייבר - אירוע השיא השנתי, שיתקיים זו השנה ה-12 בהובלת מרכז הסייבר ע"ש בלווטניק ומערך הסייבר הלאומי, מפגיש מדי שנה באירוע השיא מומחי סייבר וחוקרים מובילים מהארץ ומהעולם, לצד קובעי מדיניות, אנשי ביטחון מהארץ ומהעולם, דיפלומטים וראשי תאגידים בינלאומיים בתחום לסבב שולחנות עגולים, הרצאות, דיונים וסדנאות.

בין הכנסים והנושאים שיידונו: היבטים דיפלומטיים ושיתופי פעולה בינלאומיים, ניהול משברים, משפט וסייבר בישראל ובעולם, מגמות חדשות ופתרונות חדשניים להגנת סייבר, בינה מלאכותית, רפואה וסייבר, ענן, לוחמת סייבר, תעופה ועוד.

Cyber Week
June 27th-30th, 2022
Tel Aviv University, Israel
Yuval Ne'eman Workshop for Science, Technology and Security Tel Aviv University
ICRC Blavatnik Interdisciplinary Cyber Research Center
TEL AVIV UNIVERSITY אוניברסיטת תל אביב
Cyber Israel National Cyber Directorate
In cooperation with:
Ministry of Foreign Affairs Israel
ISRAEL CYBER ALLIANCE
State of Israel Ministry of Economy and Industry Foreign Trade Administration
ISRAEL EXPORT INSTITUTE

מקור ראשון

סייבר ניישן: ישראל מארחת את שבוע הסייבר

שבוע הסייבר השנתי יוצא לדרך ומביא לישראל את ראשי תעשיית הסייבר העולמית והמקומית

מאת **נועם אמיר** — **כ"ח בסיון ה'תשפ"ב (27/06/2022 08:51)** בתוך **חדשות**

אחד הכנסים המרתקים שהתקיימו בשנים האחרונות. אילוסטרציה. צילום: שאטרסטוק

שתף בפייסבוק | שתף בטוויטר | שתף ב- Whatsapp | שתף בדוא"ל

העולם כולו יישא עיניו לאחד הכנסים המרתקים שהתקיימו בשנים האחרונות. בכירים מהארץ ומהעולם, ממערך הסייבר הישראלי ומהבית הלבן, יתכנסו החל מהיום (ב') לשבוע הסייבר כאן בישראל, במעמד ראש הממשלה

ערוץ 7 www.inn.co.il

סגן מפקד יחידת 8200: סוכלו ניסיונות השתלטות על מערכות המים בישראל

סגן מפקד היחידה חשף טפח מפעילותה באירוע שבוע הסייבר באוניברסיטת תל אביב.

קובי פינקלר

אורי, סגן מפקד יחידת 8200 חשף בכנס הסייבר באוניברסיטת תל אביב כי היחידה סיכלה ניסיונות להשתלט על מערכות המים הקריטיות של ישראל וכן על תוקפים שניסו לפגוע בתחנות הכוח בארה"ב.

"סיכלנו את הניסיון להשתלט על מערכות המים הקריטיות של ישראל ולהרעיל אותן לפני מספר שנים. במקרה אחר זיהינו גם כי יריב מסוים תקף את ישראל ותוך כדי זיהינו שאותו תוקף ניסה גם לכוון לתחנות כוח בארה"ב. זו הייתה האינדיקציה הראשונה להתקפה זו, את האיום הזה הצלחנו למנוע באמצעות שיתוף פעולה הדוק עם השותפים האמריקאים שלנו. הישגים כאלו הם שגורמים לחיילים שלנו להיות גאים בעבודתם ב-8200", סיפר אורי.

"ל-8200 יש אחריות כלפי החברה הישראלית ואנו קולטים צעירים רבים מהפריפריה במטרה להשפיע על התעשייה. 73% מכוח האדם שלנו מתחת לגיל 23 וזה סוד הקסם של היחידה שמייחד אותנו בהשוואה לסוכנויות ויחידות בארץ ובעולם", הוסיף.

לדבריו, "כבר כמה עשרות שנים אנחנו מהווים חלק ניכר ממערך ההגנה והמודיעין של ישראל והמשימה שלנו היא איסוף מודיעין על איומים מכריעים על ישראל. ידוע לכל שאנחנו מהווים שחקן מרכזי בתחום הסייבר בישראל ומעבדים את המידע באמצעות כלים שפותחו אצלנו. המידע שאנו מקבלים מגיע ממקורות שונים משותפים, ובעיקר בזכות פעולה אקטיבית במרחב הסייבר אל מול רשתות יעד ותשתיות ארגוני טרור. אנחנו חיים בסביבה קשה וזה מצריך מאיתנו לעבוד קשה בסביבה דינמית ואינטנסיבית שמספקת אתגרים חדשים מדי יום. כשאנחנו מצליחים אנחנו מצילים חיים. כשאנחנו נכשלים זה הופך לבעיה גדולה עבור האומה שלנו".

עוד הוסיף כי "היחידה שלנו היא חלק מרכזי במערך המודיעין וההגנה של ישראל ואנחנו עובדים בשיתוף פעולה עם היחידות האחרות. סיכול איומי סייבר (CCO - Counter Cyber Operations) הוא חלק מרכזי בפעילות שלנו. מטרתנו להשיג עליונות על התוקף, להצליח לזהות אותו ולפעול כדי לשלול את יכולותיו. כך לעיתים אנו גם מוצאים קורבנות מחוץ לישראל ואז אנו יוצרים קשר עם סוכניות אחרות אם צריך. אנו עושים זאת גם באופן עצמאי וגם על ידי שיתוף פעולה עם התעשייה וסוכנויות אחרות, באמצעות יישום ושימוש בכלים שפיתחנו. 8200 לא תנוח עד שהאיום יוסר".

עוד ציין כי "דבר נוסף המחייב הדגשה הוא האחריות שיש לנו כלפי החברה הישראלית ואנחנו יודעים שלגיוון בגיוסים שלנו יש השפעה אחר כך על הגיוון בהייטק הישראלי. לצד יחידות נוספות בצה"ל הרחבנו בשנה שעברה את תכנית <גשרים> מתיכונים לחטיבות הביניים ובשנה הבאה נרחיב את התכנית ליותר מ-20 רשויות נוספות ואנחנו צופים השתתפות של יותר מ-20 אלף בני נוער. בעשור האחרון, קלטנו צעירים רבים גם מהפריפריה ואני בטוח שזה ישפיע על התעשייה והחברה גם בעשור הקרוב. רוב מה שאנחנו עושים הוא חסוי ואנחנו פועלים על מנת למנוע איומי סייבר נגד ישראל ומבטיחים שישראל תישאר מעצמה מובילה בתחום הטכנולוגיה והסייבר באזורנו. בתוך המרחה הזה יש לנו אחריות על אתיקה, מוסר וערכים ואנו לוקחים אותה ברצינות רבה, תוך שמירת מחויבות לערכים הדמוקרטיים שלנו, לנורמות במרחב הסייבר ולחברה הישראלית וזו הסיבה העיקרית שאני עומד פה היום".

ynet
ידיעות אחרונות

מתקפת הסייבר באילת: "הפורצים חדרו למערכת הכריזה ב-3 מוקדים - והשמיעו אזעקה"

החשד שהאקרים איראנים עומדים מאחורי אזעקות השווא באילת ובירושלים שוב העלה חששות מנזקים אפשריים של אירועי סייבר עתידיים. בעיריית אילת אישרו: "חשד לאירוע סייבר במערכות כריזה אזרחיות. הפגם שהוביל לפריצה אותר". ד"ר הראל מנשרי לאולפן ynet: "מערך הסייבר לא יכול להגן על הכול. צריך מודעות"

מאיר אוחיון, אלכסנדר לוקש, איתמר אייכנר

מתקפת הסייבר שלפי החשד הובילה לאזעקות השווא בירושלים ובאילת אתמול (יום ראשון), וככל הנראה בוצעה על-ידי האקרים איראנים, מעלה שוב את החששות מאירועי סייבר משמעותיים שעלולים להביא לנזקים גדולים. בעיריית אילת אישרו הבוקר את החשד לאירוע סייבר ב"מערכות כריזה אזרחיות", אך הבהירו: "אין פגיעה בצופרי פיקוד העורף בעיר".

לפי ההודעה בדיקה של מינהל אבטחת מידע בעירייה מעלה כי מדובר בפריצה למערכת הכריזה העירונית המרושתת בגני המשחקים ונועדה לשימוש מרכז השליטה העירוני למניעת ונדליזם. הפורצים השתמשו במערכת הכריזה בשלושה מוקדים, להשמעה של אזעקה עולה ויורדת. באילת הדגישו: "מדובר ברשת אינטרנטית עצמאית שאין לה שום השפעה על אבטחת המידע בעירייה ואינה קשורה כלל וכלל לרשת העירונית. הפגם שהוביל לפריצה אותר והוא מטופל מול החברה האמונה על המערכת".

שר התקשורת יועז הנדל אמר לאולפן ynet בהתייחסו לנושא: "קודם כל זו מתקפה פשוטה יחסית, אבל לצערנו גם נורא פשוט לחדור לאותן מערכות. אלו לא מערכות של פיקוד העורף אלא מערכות של השלטון המקומי. מי שמתעסק בהגנת הסייבר, והיום השלטון המקומי נכנס לזה בכל הכוח, צריך להבין שנדרש מינימום של הבנה ומינימום של הגנה, כי את החדירה לאותן מערכות היה מאוד קל לעשות, ללא קשר למי שעשה את זה.

"אנחנו יעד למתקפות סייבר של גורמים כאלה ואחרים באזור שלנו, ולכן גם לרשויות יש אחריות. אנחנו מטפלים בזה בשיתוף שב"כ, המטה ללוחמה בסייבר ומשרד התקשורת. אנחנו בתהליך של דרישת רף גבוה יותר כל יום. אנחנו מבינים שהצינורות שמעבירים את האינטרנט זה גם הצינורות שדרכם מגיעות המתקפות. לכן אנחנו מקימים פילטרים נוספים כדי לייצר בסוף סוג של כיפת ברזל סייברית".

מעיריית ירושלים נמסר כי "מדובר בחשד למתקפת סייבר במערכות הכריזה העירוניות, שנבדק ע"י מערך הסייבר הלאומי ובפיקוד העורף. מבדיקה ראשונית עולה כי אמש הופעלו המערכות בשעות הערב בכ-10 פארקים וגנים ציבוריים, במספר שכונות בעיר, ובהן נווה יעקב, בית הכרם וגוננים. אין מדובר בפגיעה במערכות אבטחת המידע העירוניות אלא ברשת אינטרנטית נפרדת שאינה קשורה למערכות העירייה".

"יש עדיין כמה לקונות בנושאי הגנה"

ד"ר הראל מנשרי, ממקימי מערך הסייבר בשב"כ, אמר הבוקר בריאיון לאולפן ynet כי המקרה האחרון הוא "לא בדיוק עליית מדרגה", אך הדגיש כי בעוד ההגנה על תשתיות קריטיות בישראל היא טובה - "יש עדיין כמה לקונות בנושאי הגנה" בארץ.

אזעקות השווא נשמעו אמש באילת, בבית שמש ובכמה שכונות בירושלים - בית הכרם, פסגת זאב ונווה יעקב. כעבור שעות, נשמעו שוב אזעקות בשכונות בירושלים. בעקבות זאת, מערך הסייבר הנחה את הרשויות המקומיות לנקוט "אמצעי הגנה מהירים על מערכות כריזה מקומיות", שכן לא מדובר במערכות ההתרעה של פיקוד העורף - אלא במערכות עירוניות.

לדברי מנשרי, "יש אירועים כאלה מדי פעם. בטוח שמי שעשה את זה לא בדיוק דורש את טובת היהודים או טובת ישראל. בהחלט צריך לדעת להתגונן מול דברים כאלה. מה שטוב במקרה הזה, שלא מדובר כאן כנראה בפריצה למערכות ממשלתיות כמו של פיקוד העורף אלא למערכת עירונית".

הוא ציין כי "במדינת ישראל יש הגנה די טובה על מערכות תשתית קריטית, תשתיות חיוניות כמו חשמל, מים ותחבורה. אין ולא תהיה אף פעם הגנה הרמטית של 100%. מדינת ישראל כבר הרבה מאוד שנים הייתה הראשונה בעולם שהסתכלה על הדברים בצורה הוליסטית והחלה להגן על עצמה מתחילת שנות האלפיים. מערך הסייבר הלאומי וגורמי הגנה נוספים לא מגנים על הכול, וחסרה הרבה מאוד מודעות בקרב גורמים עירוניים ואזוריים בצורך שלהם להגן".

על רקע הניסיונות לפרוץ גם למערכות בריאותיות, אמר ד"ר מנשרי כי "להבנתי, בפריצה שהייתה לבית החולים הלל יפה בחדרה חלק מגורמי ההגנה לא עשו דברים שהם היו צריכים ויכולים לעשות. חסרה הרבה מאוד מודעות בגורמים רשותיים ועירוניים והדבר הזה ניתן לתיקון. מתקפת סייבר יכולה להביא גם לפגיעה בחיי אדם. ראינו את זה בתקיפה שהייתה בעבר על מערך הבריאות הבריטי כשאנשים מתו.

"הציון של ישראל בהגנה על המערכות הוא בין הגבוהים בעולם. מצד שני, כשאני מסתכל על העורף הציבורי, המשק של מדינת ישראל - ארגונים ובתים כולל המקום שממנו אתם משדרים - הציון הוא לא מספיק טוב. מדינת ישראל, בגלל בעיות חוקיות בין היתר, לא השכילה עדיין לתת כלים שיאפשרו הגנה טובה ומספיקה. האזרחים צריכים לדעת ולהבין שהם חייבים להיות חלק מהמערכה ההגנתית".

מנכ"ל איגוד האינטרנט הישראלי, יורם הכהן, אמר כי "נראה שהמתקפה לא פגעה בתשתית המוגדרת בישראל כקריטית. יחד עם זאת, שוב התברר עד כמה פגיעה במערכות אזרחיות, פשוטות יחסית, משבשת את חייהם של האזרחים והאזרחיות בישראל.

"ישנו פער לא מבוטל בין יכולות הגנת הסייבר המצוינות של מדינת ישראל על תשתיות שהיא מגדירה כקריטיות לבין ההגנה הלוקה בחסר בהגנה על תשתיות אזרחיות אחרות", הסביר הכהן. "המתקפה הזאת היא לא הראשונה שמחדדת את הפער הזה. די להיזכר בפרשת הפריצה לאתר אטרף שפגעה בפרטיותם של ישראלים רבים. נדרשת הגברת מודעות ונדרש יישום אמצעי הגנת סייבר בכלל המשק".

עמרי וקסלר, חוקר במרכז למחקר סייבר באוניברסיטת תל אביב, אמר: "התקיפה אירעה על מערכות כריזה של ירושלים ואילת. העובדה שהתוקפים התמקדו במערכות של אילת, ולא נניח, של תל אביב, הנתפסת בעיני איראן ושלוחותיה כסמל ישראלי מובהק, מראה כי מדובר באופורטוניזם ולא בקמפיין מורכב ומתוכנן זמן רב מראש - ההאקרים תקפו היכן שמצאו פרצות.

"בהינתן שרוב מוחלט של תקיפות הסייבר בעולם מתמקדות במניע כספי או במטרות ריגול, הדפוס של גרימת נזק או

יצירת בהלה מתאים לפעילות האיראנית מול ישראל. התקיפות הללו אינן ייחודיות, הן חלק משגרה יומית שכוללת אלפי ניסיונות פריצה לכל מערכת או שרת שהפגיעה בו עלולה לייצר הד תקשורתי, וזאת להבדיל מפעילות ריגול שמתקיימת גם היא כל העת".

זו לא הפעם הראשונה שאירועי סייבר נגד ישראל מיוחסים לאיראן: רק בשבוע שעבר חברת אבטחת המידע צ>ק פוינט חשפה שתוקפים איראנים פרצו לתיבות מייל של גורמי מפתח בישראל והתחזו אליהם במטרה לדלות מידע מגורמים בכירים ישראליים אחרים. התוקפים התחזו לכמה בכירים, בהם אלוף בכיר במילואים ושגריר ארה"ב לשעבר בישראל, והשתמשו בזהות שלהם על מנת לדלות מידע מגורמים בכירים אחרים, בהם שרת החוץ לשעבר ציפי לבני ומנהל בכיר בחברה ביטחונית מרכזית במדינה.

תחום הסייבר הפך בשנים האחרונות לאחת הזירות המשמעותיות בעימות בין ישראל לאיראן, על רקע המאמצים לבלום את תוכנית הגרעין של הרפובליקה האיסלאמית. בחודש שעבר חשף שב"כ כי גורמי מודיעין איראנים פנו ברשת לאנשי אקדמיה, אנשי עסקים ובכירים לשעבר במערכת הביטחון - בניסיון לפתות אותם להגיע לחו"ל במטרה לפגוע בהם או לחטוף אותם.

בין תקריות הסייבר הבולטות בשנים האחרונות: ניסיון איראני שנחשף ב-ynet לתקוף מתקני מים בישראל ולהעלות את רמת הכלור, מתקפת נגד ששיתקה את הפעילות בנמל בדרום איראן, וגם פריצה איראנית לטלפון של שר הביטחון בני גנץ. כמו כן, מעת לעת קבוצות האקרים שלעיתים מקורן באיראן מצליחות לדלות מאגרי מידע משמעותיים של חברות או אנשי ביטחון, ומפרסמות מסמכים בערוצי טלגרם בדרישה לכופר.

וואלה

חשד: מתקפת סייבר איראנית גרמה לאזעקות שווא בירושלים ובאילת

מערך הסייבר הלאומי הנחה את הרשויות המקומיות לנקוט באמצעי הגנה בשל החשד כי אירוע סייבר בממשק של מערכות הכריזה לעיריות הפעיל את האזעקה, שאינה של פיקוד העורף, בבירה ובעיר הדרומית. לא נמסר מי עומד מאחורי המתקפה, אך נבדק אם מדובר בהאקרים איראנים

ינון בן שושן

חשד כי מתקפת סייבר גרמה לאזעקת שווא בירושלים ובאילת - כך מסר הבוקר (שני) מערך הסייבר הלאומי. בעקבות המקרה, המערך הנחה אמש את הרשויות המקומיות להגן על מערכות כריזה מקומיות. המתקפה לא הייתה על מערכות של פיקוד העורף ולא נמסר מי עומד מאחוריה, אך נבדק אם מדובר בהאקרים איראנים.

"ישנו פער לא מבוטל בין יכולות הגנת הסייבר המצוינות של מדינת ישראל על תשתיות שהיא מגדירה כקריטיות לבין ההגנה הלוקה בחסר בהגנה על תשתיות אזרחיות אחרות", אומר מנכ"ל איגוד האינטרנט הישראלי, יורם הכהן.

עמרי וקסלר, חוקר במרכז למחקר סייבר באוניברסיטת ת"א אשר ייקח חלק בשבוע הסייבר השנתי, התייחס לאירוע ואמר כי "העובדה שהתוקפים התמקדו במערכות של אילת, ולא נניח, של תל אביב, הנתפסת בעיני איראן ושלוחותיה כסמל ישראלי מובהק, מראה כי מדובר באופרטוניזם ולא בקמפיין מורכב ומתוכנן זמן רב מראש - ההאקרים תקפו היכן שמצאו פרצות".

"אירוע של הפעלת אזעקות כפי שאירע אתמול יכול לייצר בהלה בקרב הציבור שאינו מבחין בין מתקפת סייבר שיכולה להעמיד את המדינה בסכנה, לבין מתקפה שכזו שמטרתה על פניו היא שיבוש סדר היום ופגיעה באמון הציבור", אומרת מיי ברוקס קמפלר, מומחית סייבר, בשיחה עם וואלה! טכנולוגיה. "החשש במערכת הביטחונית במקרה זה צריך להיות

כפול - הן החשש מפני חוסר אמון הציבור במערכות האזעקה והתעלמות מהן באירוע אמת עתידי אשר עשוי חלילה להביא לפגיע בחיי אדם, והן התרחיש על פיו מדובר בהוכחת יכולת של האויב לקראת שיבוש מערכי האזעקות בזמן מלחמה במרחב הפיזי".

בשבוע שעבר פרסמה חברת אבטחת הסייבר הישראלית צ>ק פוינט על מהלך תקיפה איראני נגד גורמים בכירים בישראל, שהחלה בדצמבר 2021, ובהם שרת החוץ לשעבר ציפי לבני. כחלק מהמתקפה, פרצו ההאקרים לתיבת מייל של אלוף בכיר במילואים ששימש בתפקיד רגיש, התחזו אליו והתכתבו בשמו עם גורמים בכירים במטרה לגרום להם לפתוח מסמכים שונים. צ>ק פוינט עדכנה את גורמי הביטחון בישראל על המתקפה.

על פי המחקר, ניהלו תוקפים איראנים תכתובות מייל עם גורמים בכירים בישראל לאחר פריצה למספר כתובות מייל והתחזות לאותם הגורמים. התכתובות כללו שליחת מסמכים הכוללים הזמנה לכנס בחו"ל ומאמרים בנושא תכנית הגרעין האירנית - ואלו דרשו מהקורבנות להקליד את סיסמת המייל שלהם. באחד מהמקרים התכתובות הובילו מנהל בכיר באחת החברות הבטחוניות המרכזיות בישראל לשלוח את צילום הדרכון שלו.

במהלך חודש דצמבר קיבלה שרת החוץ לשעבר לבני מספר מיילים בעברית מאותו אלוף במילואים, ובהם ביקשה לקרוא מאמר שכתב על אירועים ביטחוניים בשנת 2021. לאחר כמה מיילים שבהם הפציר בלבני לפתוח את הקובץ באמצעות סיסמת המייל שלה, לבני פנתה לאותו אלוף במילואים שלא הבין במה מדובר.

"לבני העבירה אלינו את תכתובת המיילים, וממנה התחקנו אחר השולחים והקבצים וגילינו עד כמה רחב היה המהלך (פרסום שמה של לבני תואם איתה)", מסרו בחברת צ>ק פוינט. לדבריהם, באותם החודשים ועד לשבוע שעבר, התוקפים האיראנים הצליחו לשים את ידם על תכתובת מייל פרטית בין ראש מכון מחקר מרכזי מאוד בישראל ושגריר ארה"ב לשעבר בישראל, וניצלו אותה ליצירת המשך התכתבות במהלכה הם התחזו לשגריר תוך שימוש במייל אחר.

ישראל היום
הכי ישראלי כל הזמן

חשד: מתקפת סייבר איראנית גרמה לאזעקות שווא בירושלים ובאילת

מערך הסייבר הלאומי הנחה את הרשויות המקומיות לנקוט באמצעי הגנה בשל החשד כי אירוע סייבר בממשק של מערכות הכריזה לעיריות הפעיל את האזעקה, שאינה של פיקוד העורף, בבירה ובעיר הדרומית. לא נמסר מי עומד מאחורי המתקפה, אך נבדק אם מדובר בהאקרים איראנים

ינון בן שושן

מערך הסייבר הלאומי הנחה אמש (ראשון) את הרשויות המקומיות לנקוט אמצעי הגנה מהירים בכדי לשמור על מערכות הכריזה המקומיות. זאת, לאור חשד לאירוע סייבר בממשק של מערכת כריזה לעיריות אשר הביא להפעלת הכריזה במספר קטן של נקודות בערים אילת וירושלים. יודגש כי המערכות אינן מערכות ההתרעה של פיקוד העורף.

בעיריית אילת עידכנו כי אכן מדובר בחשד לאירוע סייבר במערכות כריזה אזרחיות וכי צופרי פיקוד העורף בעיר לא נפגעו. בדיקה של מנהל אבטחת מידע בעירייה העלתה כי מדובר בפריצה למערכת הכריזה העירונית המרושתת בגני המשחקים ונועדה לשימוש המשל"ט העירוני למניעת ונדליזם.

הפורצים השתמשו במערכת הכריזה בשלושה מוקדים - בגן משחקים ברובע 6, בפארק הספורט ביעלים ובמועדון השיט בחוף הצפוני, להשמעה של אזעקה עולה ויורדת. לטענת העירייה, הפגם שהוביל לפריצה אותר והוא מטופל מול החברה האמונה על המערכת.

מנכ"ל איגוד האינטרנט הישראלי, יורם הכהן, אמר בתגובה לחשד לתקיפת הסייבר: "נראה שהמתקפה לא פגעה בתשתית המוגדרת בישראל כקריטית. יחד עם זאת, שוב התברר עד כמה פגיעה במערכות אזרחיות פשוטות יחסית, משבשת את חייהם של האזרחים בישראל. ישנו פער לא מבוטל בין יכולות הגנת הסייבר המצוינות של מדינת ישראל על תשתיות שהיא מגדירה כקריטיות לבין ההגנה הלוקה בחסר על תשתיות אזרחיות אחרות. המתקפה הזאת היא לא הראשונה שמחדדת את הפער הזה - די להיזכר בפרשת הפריצה לאתר אטרף שפגעה בפרטיותם של ישראלים רבים. נדרשת הגברת מודעות ויישום אמצעי הגנת סייבר בכלל המשק".

לאירוע החריג התייחס גם ד"ר הראל מנשרי, ראש תחום סייבר בHIT מכון טכנולוגי חולון, וממקימי מערך הסייבר בשב"כ: "התוקפים ניסו להראות שהם יכולים להטריל ולהכניס את הציבור הישראלי לפאניקה וללחץ. אני לא מתרגש מהתקיפה הזו יותר מדי מהסיבה שלא מדובר על תקיפה על מערכת ממשלתית קריטיות אלא על מתקפה על רשויות מקומיות. התקיפה הזו היא סוג של קריאת השקמה, יש כאן סוגייה שבהחלט צריכים להתייחס אליה. תשתיות ממשלתיות קריטיות זוכות להגנה ברמה טובה אבל ברשויות המקומיות, ההגנה לא ברמה מספקת וגם המודעות של המשתמשים במערכות לסיכונים לא מספיק טובה. מדינת ישראל צריכה להקצות יותר משאבים כדי לספק הגנה יותר טובה לגופים ציבוריים".

עמרי וקסלר, חוקר במרכז למחקר סייבר באוניברסיטת ת"א, שייקח חלק בשבוע הסייבר השנתי, אמר: "התקיפה אירעה על מערכות כריזה של ירושלים ואילת. העובדה שהתוקפים התמקדו במערכות של אילת, ולא נניח, של תל אביב,

PC אנשים ומחשבים

"הערך היחיד שהאיראנים השיגו ממתקפת הסייבר – שמדברים עליה"

המתקפה, שהפעילה אזעקות בי-ם ובאילת, היא הצלחה איראנית, אבל לא משמעותית - סבור עמרי וקסלר, חוקר סייבר בכיר באוניברסיטת תל אביב● הוא מסביר לאנשים ומחשבים את המתקפה ומה צריך לעשות כדי שהיא לא תקרה שוב

יניב הלפרין

מתקפת הסייבר, שבמסגרתה חדרו האקרים איראניים למערכות הכריזה של עיריות אילת וירושלים והפעילו אזעקות שווא בכמה מוקדים בהן, היא לא אירוע משמעותי, אולם כזה שמחייב חשיבה מחדש וניסוח מדיניות סייבר בכל הנוגע לרשויות המקומיות – כך סבור עמרי וקסלר, חוקר בכיר במרכז למחקר סייבר באוניברסיטת תל אביב. "הנזק של האירוע הזה הוא תודעתי, הבהלה שהוא גרם בשכונות שבהן הופעלו האזעקות, והעובדה שמדברים על זה", הוא ציין בראיון לאנשים ומחשבים.

וקסלר, שייקח חלק בשבוע הסייבר הלאומי, שיתקיים בשבוע הבא, הערך שהמתקפה לא בוצעה על ידי האקרים מהמודיעין האיראני או משמרות המהפכה. מבצעיה, לדבריו, הם "אזרחים פטריוטים שמקושרים לאחד מארגונים אלה, או לבאסיג>, שאלה מיליציות חצי אזרחיות וחצי צבאיות". הוא אמר שההאקרים הצליחו במתקפה, אבל בצורה מוגבלת בלבד, שכן לא הופעלו אזעקות בתל אביב, שהיא "הסמל הישראלי המובהק" בעיני האיראנים.

אבל הם הצליחו להפעיל אזעקות בירושלים, בירת ישראל.

"נכון, אבל לתפיסתם, ירושלים לא שייכת לישראל. כשהם מאיימים על ישראל, הם תמיד מדברים על תל אביב".

הנתפסת בעיני איראן ושלוחותיה כסמל ישראלי מובהק, מראה כי מדובר באופרטוניזם ולא בקמפיין מורכב ומתוכנן זמן רב מראש - ההאקרים תקפו היכן שמצאו פרצות. בהינתן שרוב מוחלט של תקיפות הסייבר בעולם מתמקדות במניע כספי או במטרות ריגול, הדפוס של גרימת נזק או יצירת בהלה מתאים לפעילות האיראנית מול ישראל. התקיפות הללו אינן ייחודיות. הן חלק משגרה יומית שכוללת אלפי ניסיונות פריצה לכל מערכת או שרת שהפגיעה בו עלולה לייצר הד תקשורתי, וזאת להבדיל מפעילות ריגול שמתקיימת גם היא כל העת".

בנוסף, סגן שרת הכלכלה, ח"כ יאיר גולן, התייחס לאירועים בראיון לגל"צ: "היו ניסיונות רבים של האיראנים לפגוע בישראל דרך הסייבר, נערכים לזה בצורה רצינית. לא נפרצה מערכת האזעקות של פיקוד העורף, אלא מערכות כריזה מקומיות, אך זה מדאיג ומטריד מאוד - אם יש פה פרצה, צריך לסגור אותה מיד".

האם אתה מעריך שהם ניסו לחדור למערכות בתל אביב?

"אי אפשר לדעת, אם כי בהחלט ייתכן שהם ניסו לחדור למערכות הכריזה של תל אביב, ונתקלו בקשיים. נראה שהם ניסו לחדור למערכות של כל מיני ערים, והצליחו באילת".

"זה לא נראה כמו מבצע איראני מורכב ומתוכנן", אמר וקסלר, "אלא כמשהו שנועד ליצור בהלה ופאניקה בקרב אזרחים. זו מתקפה של הפרעה ושיבוש ולא מתקפה קריטית כמו הפריצה למערכת המים של ישראל, שבוצעה ב-2020. לא נגרם הפעם נזק משמעותי".

המערכות שהאיראנים חדרו אליהן הן של רשויות מקומיות ולא של פיקוד העורף. איך אתה מסביר את הפער?

"הם ניסו ב-2019 לפרוץ למערכות של פיקוד העורף, ולא הצליחו. יש גופים שמידת ההגנה שלהם הרבה יותר גבוהה ומוכחת, כגון מערכות של צה"ל ותשתיות קריטיות. כנראה שיש פער במודעות לאיום ופער בהיערכות, ולכן אנחנו <חוטפים> בתשתיות עירוניות ובגופים פרטיים.

הפער הזה קיים בכל העולם. אף גוף הגנת סייבר לאומי לא יכול להגן על הכול. גם בישראל, שהייתה הראשונה שהקימה גוף שכזה, וגם בשאר העולם, גופי הסייבר אחראיים להגנה קודם כל על התשתיות הקריטיות.

בנוסף, הרגולציה על ארגונים שאינם תשתיות קריטיות לוקה בחסר. חשוב לזכור בהקשר זה שמערך הסייבר הלאומי הוא גוף מנחה ולא גוף אכיפה. צריך לתת יותר חשיבות להגנה על ארגונים כמו הרשויות המקומיות, שהותקפו כאן".

אתה אומר שלא היו פגיעות משמעותיות. זה נכון ברמה של דליפת נתונים או ביטחון המדינה, אבל אזעקות יכולות לגרום ללחץ ואף פאניקה אצל אנשים.

"אמת, ולבי עם אנשים עם פוסט טראומה שאזעקות כאלה יכולות להשפיע עליהן או מבוגרים שמחליקים בדרך למקלט לאחר הישמע אזעקה, וצריך לתת על זה את הדעת, אבל יש להבדיל בין זה לבין תקיפות שיכולות להשתיק בית חולים או להוריד את רשת החשמל – מה שעלול להוות סכנת חיים".

מה צריך לעשות כדי למנוע הישנות של מקרים כמו זה?

"הסייבר ברשויות המקומיות הוא לקונה שצריך להיכנס אליה, יש לפקח עליהן יותר בהיבט זה, לנסח דרישות אבטחה יותר נוקשות ולאכוף אותן. הבעיה היא רחבה הרבה יותר, כי זה עניין של אכיפה לא רק על הרשויות המקומיות. למרבה האבסורד, גם בתי החולים לא מוגדרים תשתיות קריטיות, וראינו תוצאה של זה במתקפה על בית החולים הלל יפה, שנגרמה בגלל שירות VPN שלא עודכן, מה שהביא להחדרת חולשה מ-2018. אחת הדרכים להגברת הרגולציה יכולה להיות חוק הסייבר, שתקוע בממשלה כבר כמה שנים. אלא שנראה שבגלל המצב הפוליטי, הוא לא יקודם גם בחודשים הקרובים".

סגן מפקד 8200: "כשאנחנו נכשלים זה הופך לבעיה גדולה"

סגן מפקד יחידת 8200 התארח בכנס הסייבר באוניברסיטת תל אביב והתייחס לאיומים האיראנים, לאתגרי הגיוס וגם סיפק הצצה מפציעה לפעילות היחידה המסווגת.

סגן מפקד יחידת 8200, אורי (שמו המלא אסור לפרסום) התארח הבוקר (יום ד') בשבוע הסייבר השנתי בהובלת המרכז למחקר סייבר באוניברסיטת ת"א, מערך הסייבר הלאומי, משרד הכלכלה ומשרד החוץ. במסגרת הכנס מפקד 8200 נשא דברים לראשונה בפני קהל: "זוהי ההופעה הפומבית הרשמית הראשונה של 8200".

בדבריו התייחס אורי לאתגרים היומיומיים ואמר: "כשאנחנו מצליחים אנחנו מצילים חיים. כשאנחנו נכשלים זה הופך לבעיה גדולה עבור האומה שלנו. מטרתנו היא להשיג עליונות על התוקף, להצליח לזהות אותו ולפעול כדי לשלול את יכולותיו. 8200 לא תנוח עד שהאיום יוסר".

בדבריו תיאר סגן מפקד היחידה מקצת מהפעולות שהיחידה עשתה בשנים האחרונות: " סיכלנו את הניסיון להשתלט על מערכות המים הקריטיות של ישראל ולהרעיל אותן לפני מספר שנים. במקרה אחר זיהינו גם כי יריב מסוים תקף את ישראל ותוך כדי זיהינו שאותו תוקף ניסה גם לכוון לתחנות כוח בארה"ב. הישגים כאלו הם שגורמים לחיילים שלנו להיות גאים בעבודתם ב- 8200".

אורי גם התייחס לאתגרי הגיוס ליחידיה והניסיון לגוון ולפתוח את שערי היחידה לכלל החברה הישראלית: " ואנחנו יודעים שלגיוון בגיוסים שלנו יש השפעה אחר כך על הגיוון בהייטק הישראלי. קלטנו צעירים רבים גם מהפריפריה ואני בטוח שזה ישפיע על התעשייה והחברה גם בעשור הקרוב".

קול חי תמיד אתך! 93/92.8FM ▶ 93fm.co.il

ראש מערך הסייבר: "מקדמים כיפת סייבר להגנה על המשק"

ראש מערך הסייבר הלאומי גבי פורטנוי נשא דברים בשבוע הסייבר ואמר: "אנו מקדמים כיפת סייבר לחיזוק ההגנה על המשק כולו. איראן היא שחקן מרכזי שאנחנו מזהים במרחב" | על פי נתוני מערך הסייבר הלאומי שהוצגו בכנס, בשנה האחרונה בלם המערך כ-1,500 ניסיונות תקיפה העורף הישראלי

קובי פינקלר

בנאום מקיף ראשון מאז כניסתו לתפקיד לפני כארבעה חודשים, הציג היום גבי פורטנוי, ראש מערך הסייבר הלאומי את הפרויקט החדש של המערך ליצירת כיפת סייבר על המרחב האזרחי. בהתייחס לתוקפים במרחב אמר פורטנוי כי: "איראן הפכה לשחקן מרכזי שאנו מזהים במרחב הסייבר, יחד עם חמאס וחיזבאללה. אנחנו רואים אותם, אנחנו יודעים איך הם עובדים ואנחנו שם". את הדברים הציג פורטנוי בכנס כחלק משבוע הסייבר, שמתקיים השבוע בהובלת מערך הסייבר הלאומי והמרכז למחקר סייבר באוניברסיטת תל אביב.

על פי נתוני מערך הסייבר הלאומי שהוצגו בכנס, בשנה האחרונה בלם המערך כ-1,500 נסיונות תקיפה שונים על העורף הישראלי. לדברי פורטנוי בכנס, "למערך יש נקודת תצפית ייחודית על ההגנה המדינתית. אנחנו עוברים להסתכלות מגזרית על המשק – הסתכלות על פי תחומים ולא על פי גופים. אנחנו עוברים מפרדיגמה שמסתכלת על התוקף לפרדיגמה שמסתכלת על העורף האזרחי".

בהתייחס לסוגי התוקפים אמר, "מגוון התוקפים בזירת הסייבר הורחב וכולל גם תוקפים נוספים, קבוצות תקיפה, שלוחות של מדינות, ארגוני פשיעה, אנשים פרטיים ועוד".

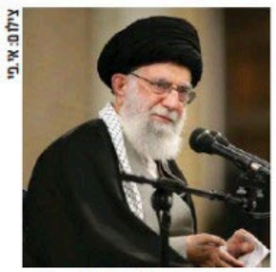
בהמשך דבריו הציג פורטנוי את הפתרון החדש שמקדם המערך להגנה על המשק: "אנחנו צריכים כיפת ברזל הגנתית בתחום הסייבר לטובת אזרחי מדינת ישראל. כיפת הסייבר היא פרויקט הדגל החדש שלנו במערך לחיזוק הגנת הסייבר של המשק כולו. הפרויקט יעשה שימוש במנגנונים חדשים ויביא לצמצום מתקפות הסייבר בצורה משמעותית. כיפת הסייבר היא גישה פרו-אקטיבית חדשה לחיזוי ובלימת מתקפות שמשלבת טכנולוגיות של ביג-דאטא ובינה מלאכותית".

פורטנוי הציג את ההרחבה של הכלים של המערך ופתיחתם מהטמעה בתשתיות הקריטיות בלבד לסקטורים ותחומים נוספים. לסיכום אמר כי "רק באמצעות שיתוף פעולה – בין מדינות, עם חברות הגנת הסייבר, האקדמיה, הממשל וגופי הביטחון – נוכל להגן על עצמנו במלחמת הסייבר וליצור כיפת ברזל הגנתית בסייבר רחבה".

ישראל היום הכי ישראלי כל הזמן

מתקפת סייבר – ומו"מ

קבוצת האקרים תקפה מפעל פלדה גדול באיראן – וגרמה לתקלות ולפיצוץ עז ● בינתיים גורמים בקטאר הודיעו: "נארח שיחות בין טהרן לוושינגטון"



עלון: א"פ

הבן ירש את האב? חמינאי

צילום: מתוך סרטון

נזק אדיר. הפיצוץ במפעל הפלדה "חוזסטאן"

נטע בר ודמיאן פצ'טר

איראן חיזדחה אתמול על כוונת קפת סייבר נגד אחד ממפעלי הפלדה הגדולים ביותר שלה, ואף שלטענתה הצליחה לסכל את רוב התקפה – היא מפרה כי חייצור בו הופסק.

ההאקרים העלו לרשת סרטון שבו נראה מתקן התכה של מתכות כבדות במפעל של חברת הפלדה "חוזסטאן" הפועלת בדרום המדינה. קבוצת ההאקרים, המכנה את עצמה "הדרדור הטורף", טענה כי פרצה לעוד שני מפעלי פלדה נוספים וגרמה גם בהם לנזקים כבדים.

בהודעה שפרסמה חברת "חוזסטאן" נאמר כי הוחלט לעצור את הפעילות במפעל עד להודעה חדשה, "בשל בעיות טכניות" שנגרמו מאותה מתקפת סייבר.

מנכ"ל החברה, אמין איברהימי, טען שהחברה הצליחה לסכל את מתקפת הסייבר ולמנוע נזק מבני לקו הייצור, נזק שהיה יכול להשפיע על שרשראת ההספקה ועל יכולת החברה לעמוד בהתחייבויות שלה ללקוחותיה.

עמרי וקסלר, חוקר בכיר במרכז הסייבר של אוניברסיטת ת"א, טוען: "למרות קבלת האחריות, קשה ומורכם סמך שנתתם ב-2015.

מוחמד מראנדי, חבר פרלמנט איראני המעורה בסוגיית שיחות הגרעין, אמר לסוכנות הידיעות "איסנא" כי איראן בחרה לקיים את השיחות בקטאר משום ש"קטאר תמיד היתה ידידה שלנו".

גם דובר משרד החוץ האיראני, סעיד חטיבזאדה, התבטא בסוגיית שיחות הגרעין, אמר כי איראן מוכנה להתקדם לעבר "הסכם צורך" וטען כי בכל הנוגע לפריצת דרך בשיחות "הכדור נמצא במגרש האמריקני".

סיוע לא צפוי

בה בעת, גורמים רשמיים בקטאר מסרו לסוכנות הידיעות "דוידרס" כי הנסיכות המפרצית תארח שיחות לא ישירות בין ארה"ב לבין איראן במסגרת המו"מ לחזרה להסכם הגרעין, זאת כדי להגיע לפריצת דרך שתאפשר התקדמות בשיחות בווינה והגעה להסכם שישיב את ארה"ב למסגרת הסכם הגרעין.

האייתוללה לעתיד

בתוך כך, ערוץ החדשות בפרסית "איראן אינטרנשיונל" ציטט שני גורמים במשטר האיראני המצביעים על מאבק מר אשר תפס תאוצה לאחרונה סביב יורשו של המנהיג העליון, האייתוללה עלי חמינאי.

לפי הדיווח, "חוסיין טאיב, שהודח בשבוע האחרון מתפקידו כראש המודיעין של משמרות המהפכה, הוא חברו הקרוב ביותר של מוג'תבא חמינאי, בנו של המנהיג העליון בן ה־83, ועובד בכל הכוח כדי להכתיר אותו כמנהיג הבא של איראן, אחרי מות אביו", נכתב.

כלי התקשורת, בעל הקו האנטי־ממסדי שיושב בלונדון, מפרט כי "טאיב אפילו גרם לבחירתו של איברהים ראיסי כדי להבשילו, ובסר פו של דבר להרחיק אותו ממועמדות אפשרית למנהיג הבא של איראן".

<tech12>

תקיפות ותגובות במרחב הסייבר מגיחות אל אור הזרקורים

השיח על השימוש ביכולות סייבר התקפיות ואף על הפיתוח שלהן ועל מקרים בהם משתמשים בהן – הופך לציבורי יותר ויותר בשנים האחרונות. מה הן ההשלכות על ההרתעה והאם הגיע הקץ לעמימות?

עומרי וקסלר

בראיון שהעניק בתחילת יוני לערוץ סקיי ניוז הודיע ראש הסוכנות האמריקנית לביטחון לאומי (NSA) ומפקד פיקוד הסייבר, גנרל פול נאקאסונה, כי ארה"ב קיימה שורת מבצעי סייבר, ביניהם מבצעי סייבר התקפיים, כחלק מתמיכתה באוקראינה. אין מדובר בפעם הראשונה בה בכירים אמריקניים מדברים בגלוי על מבצעים ותקיפות סייבר שניהלה ארה"ב כנגד יריבותיה.

השיח על השימוש ביכולות סייבר התקפיות ואף על הפיתוח שלהן ועל מקרים בהם ישתמשו בהן – הופך לציבורי יותר ויותר בשנים האחרונות. עוד ועוד מדינות מערביות מתחילות לדון בנושא זה ולשלב יכולות אלו במדיניותן. ב-2020 הקימה בריטניה את כוח הסייבר הלאומי, המתמקד במבצעים ובלוחמת סייבר כנגד גורמי טרור והאקרים הפועלים בחסות מדינות זרות. הקמת הכוח וכן דיונים על יכולותיו, משימותיו והתקציב הדרוש לו – זכו להד תקשורתי נרחב ואף להתייחסויות רשמיות מצד בכירים. דיון דומה מתקיים בשנתיים האחרונות באוסטרליה סביב השקעות נרחבות ביכולות סייבר התקפיות, במשימותיהם של גופי המודיעין להשבית תשתיות של גורמי טרור ועבריינ סייבר ובמתן מענה להתעצמות הצבאית של סין באזור דרום מזרח אסיה והאוקיאנוס השקט.

הגם שמרבית הפעילות ההתקפית במרחב הסייבר נותרת בצללים, חשיפה ציבורית ותקשורתית זו משמעותית משום שהיא מציבה את יכולות הסייבר הלאומיות של המדינות, תחום שמקורו בעולמות הביון והמודיעין, תחת אור הזרקורים. עם זאת מדינות רבות אחרות, וביניהן ישראל, שומרות במידה רבה על תרבות העמימות והתייחסות רשמית ליכולותיה ההתקפיות במרחב הסייבר נדירות.

מכאן עולה השאלה האם חשיפה, או לחלופין עמימות, משרתות את ההרתעה? נושא זה יידון בהרחבה בשבוע הסייבר השנתי של המרכז למחקר סייבר באוניברסיטת ת"א, שמתקיים השבוע. לשם כך, יש להבין את יתרונותיה וחסרונותיה של כל אסטרטגיה: שמירה על עמימות, המייחדת מאוד את מרחב הסייבר ומתאפשרת עקב השוני שבינו לבין המרחב הפיזי, מאפשרת לתוקף לשמור על מרחב הכחשה ולהימנע מתגובת היריב. מצד שני, ראיות שנאספו מתקיפות סייבר בעשור האחרון אינן מצביעות על כך שתקיפות סייבר בהכרח מובילות להסלמה בהשוואה למרחב הפיזי ואף פחות.

לעומת זאת, הכרזה, לקיחת אחריות או השארת רמזים מאפשרת לתוקף לאותת ליריב על היכולת לפגוע או להעניש אותו. מצד שני, האתגר הגדול של הרתעה, הנכון גם להרתעה במרחב הפיזי, הוא שלרוב אי אפשר לדעת האם היא משיגה את מטרתה או שסיבה אחרת מונעת מהיריב מלפעול.

סוגיה נוספת שבאה לידי ביטוי בהחלטה לחשוף מבצעי סייבר נוגעת לקהל הפנימי ומטרתה להראות לציבור שנבחריו מגיבים לתקיפות בעוצמה. דוגמה לכך היא הודעתם של בכירים אמריקנים כי בכוונת ממשל ביידן להגיב בשורת מבצעי סייבר בתגובה על הפריצה לתוכנת חברת SolarWinds שנחשפה בדצמבר 2020 וזרכה פרצו האקרים המשויכים לגופי המודיעין של רוסיה לתשע סוכנויות פדראליות וליותר מ-100 חברות פרטיות.

להכרזות אלו עשוי להיות קהל נוסף – מדינות בעלות ברית. הדבר בא לידי ביטוי כשמדינה מקיימת מבצע סייבר התקפי הנעזר בתשתיות של מדינה צד-שלישי, ועלול לפגוע בנכס מודיעיני או "להתנגש" עם מבצע לאיסוף מודיעין של מדינה בעלת ברית. דוגמאות לכך הן ציטוטים שיוחסו לבכירים אמריקנים בעיתוני הוושינגטון פוסט והניו יורק טיימס ושחשפו מתקפות סייבר ומבצעים חשאיים שקיימה ישראל כנגד תכנית הגרעין האיראנית. דוגמה נוספת היא תקיפת הסייבר שהובילה לשיבוש פעילות נמל <השהיד רג>אי> שלחופי מיצרי הורמוז באיראן במאי 2020. לדברי בכירים אמריקנים וזרים שצוטטו בעילום שם, ישראל ביצעה את המתקפה כתגובה על ניסיונם של האקרים איראנים לפרוץ למערכות המים בגליל ובמטה יהודה חודש לפני כן.

יש לזכור כי סוגיית ההחלטה אם לחשוף ולהכריז על מתקפות סייבר, לרמוז עליהן ולהדליפן לעומת ההחלטה לשמור על עמימות – היא רק חלק מהדיון על הרתעה. סוגיות נוספות, שהופכות לסבוכות יותר במרחב הסייבר בהשוואה למרחב הפיזי, נוגעות לבחירת המטרה הספציפית שתקיפתה מתאפשרת הודות למצב האבטחה שלה ושתעביר מסר. אתגר נוסף הוא הניסיון לשלוט במידת הנזק. אתגרים אלו ואחרים צפויים להמשיך ולהעסיק את מקבלי ההחלטות בעתיד הנראה לעין.

PC אנשים ומחשבים

השקעות, סייבר וקוקטייל עסקי

המתקפה, שהפעילה אזעקות בי-ם ובאילת, היא הצלחה איראנית, אבל לא משמעותית - סבור עמרי וקסלר, חוקר סייבר בכיר באוניברסיטת תל אביב הוא מסביר לאנשים ומחשבים את המתקפה ומה צריך לעשות כדי שהיא לא תקרה שוב

קרן ההשקעות YL Ventures, שמשקיעה בחברות סייבר ישראליות בשלבים מוקדמים, ערכה באחרונה קוקטייל עסקי, והזמינה אליו יזמי סייבר ובכירים בתחום בארצות הברית ובישראל.

במסגרת האירוע נערך פאנל בהנחיית יואב לייטרסדורף, מייסד ושותף מנהל בקרן, שעסק בחוסר היציבות בשוק ובהשפעתו על תעשיית הסייבר מנקודת מבטם של המשקיעים, היזמים ומנהלי אבטחת המידע בחברות מובילות. השתתפו בו אודי מוקדי, מנכ"ל ומייסד סייבארק; טימות>י בראון, סמנכ"ל אבטחת המידע של סולארווינדס, שחוותה את אחת ממתקפות הסייבר הגדולות ביותר בשנים האחרונות; טוד וובר, שותף תפעול וסמנכ"ל הטכנולוגיות של קרן הון-הסיכון טן אילבן ונצ>רס; ריצ>ארד סייוואלד, מייסד ושותף מנהל בקרן אבולושן אקוויטי פרטנרס; וגרג סאנדס, מייסד ושותף מנהל בקרן קוסטנואה ונצ>רס.

במסגרת הפאנל הדגישו המשתתפים כי תקיפות הסייבר יימשכו ואף יהפכו רבות ומתוחכמות יותר, ולכן נמשיך לראות צורך אקוטי בפתרונות טכנולוגיים מתקדמים. לכן, אמרו, על יזמים ומשקיעים לראות בתקופת התיקון הנוכחית הזדמנות לחזק את היסודות של החברות ולהקשיב לצרכי הלקוחות לקראת העשור הבא, שאותו אפיין אחד המשתתפים כ-"תור הזהב של אבטחת הסייבר".

בין היתר, לקחו חלק באירוע דורית דור, סמנכ"לית מוצר בצ>ק פוינט; גילי דרוב היישטיין, מנכ"לית המרכז למחקר סייבר באוניברסיטת תל אביב; רוי ארליך, מנכ"ל אנזו סקיוריטי; יוני שוחט, מנכ"ל ויילנס סקיוריטי; ומנכ"לי ומייסדי חברות סטארט-אפ שונות.

כלכליסט

מתקפת סייבר השביתה את פעילותה של חברת ענק לייצור פלדה באיראן

חברת חוזסטן סטיל, שבבעלות המדינה, דיווחה על הפסקת ייצור הפלדה עד להודעה חדשה בעקבות המתקפה שכוונה אליה. עם זאת, מנכ"ל החברה טוען שהיא הצליחה לעצור את המתקפה ולא נגרמו נזק לקווי הייצור - מה שהיה מוביל לפגיעה בשרשראות האספקה

אחת מחברות ייצור הפלדה הגדולות באיראן אמרה היום שהיא נאלצה להפסיק את הייצור לאחר שנפגעה ממתקפת סייבר, שהיתה כנראה אחת הגדולות ביותר נגד המגזר התעשייתי במדינה בשנים האחרונות. חברת חוזסטן סטיל, שבבעלות המדינה, דיווחה שמומחים קבעו כי על המפעל להפסיק לפעול עד להודעה חדשה "עקב בעיות טכניות" בעקבות "מתקפת סייבר". אתר האינטרנט של החברה הפסיק גם כן לפעול.

מנכ"ל החברה אמין איברהימי טען שהחברה הצליחה לעצור את המתקפה ולמנוע נזק מבני לקווי הייצור - נזק שהיה משפיע על שרשראות האספקה ועל הצרכנים. "למרבה המזל המתקפה נכשלה", כך ציטטה סוכנות הידיעות מאהר את איברהימי, שטען שאתר האינטרנט יתוקן ושהחברה ככלל תחזור לפעול כרגיל עד סוף היום. ערוץ טלוויזיה מקומי דיווח כי המתקפה נכשלה כיוון שהמפעל במקרה לא פעל בזמן הפסקת החשמל שנגרמה.

החברה לא האשימה שום גורם במתקפה, שמהווה רק את הדוגמה האחרונה לשורת מתקפות מהזמן האחרון שנועדו לפגוע בתשתיות המדינה והביכו את הרשויות. במתקפה גדולה שאירעה בשנה שעברה נגד רשת הפצת הדלק של המדינה שותקו מספר תחנות דלק ברחבי המדינה - מה שגרר זעם מצד נהגים שנאלצו לעמוד בטורים ארוכים כדי לתדלק. מתקפות נוספות כוונו נגד תחנות רכבת באיראן, מצלמות אבטחה, אתרים של גופי המדינה ועוד.

איראן האשימה את ארצות הברית ואת ישראל במתקפות. היא ניתקה חלק גדול מהתשתית הממשלתית שלה מהאינטרנט לאחר השתלת וירוס המחשב סטאקסנט במערכותיה - פעולה שיוחסה על ידה לארצות הברית ולישראל, ופגעה בפעילותן של אלפי צנטריפוגות שהן חלק מתוכנית הגרעין שלה.

ישראל היום
הכי ישראלי כל הזמן

חשד: מתקפת סייבר איראנית גרמה לאזעקות שווא בירושלים ובאילת

מתקפת קבוצת הפצחנים "הדרור הטורף" השביתה את אחד מקומפלקסי התעשייה הכבדה החשובים ברפובליקה האסלאמית • ההאקרים התחברו למצלמות האבטחה ופרסמו את צילומי הנזק שגרמו למתקן, השייך למשמרות המהפכה

נטע בר

האקרים פרצו לאחד ממעלי הפלדה הגדולים באיראן, השייך למשמרות המהפכה, ותיעדו את הנזק שגרמו למתקן התכה במקום, כך דיווח היום (שני) אתר החדשות האיראני הפועל בלונדון "איראן אינטרנשיונל".

הפצחנים העלו לרשת סרטון בו נראה מתקן התכה של מתכות כבדות במפעל של חברת הפלדה "חוזסטאן" הפועלת בדרום המדינה. קבוצת ההאקרים, המכנה את עצמה "הדרור הטורף", טענה כי פרצה לעוד שני מפעלי פלדה נוספים וגרמה גם בהם נזקים כבדים.

בסרטון שפרסם הארגון והופץ על ידי אתר החדשות האיראני נראה מתקן התכה במפעל בדרום המדינה כשהוא יוצא משליטה וגורם לשריפה קשה במקום. הרשויות באיראן הודיעו על סגירת המפעל עד הודעה חדשה.

עמרי וקסלר, חוקר בכיר במרכז הסייבר של אוניברסיטת ת"א טוען:"למרות לקיחת האחריות, קשה ומוקדם לדעת מטעם מי פועלת קבוצת ההאקרים. לא מן הנמנע כי מדובר בקבוצות האקטיביסטים או מתנגדי משטר שפועלות באיראן ומחוצה לה. תקיפות רבות פחות משמעותיות יוחסו בעבר גם לארגון מוג>הידין א-חלק, ארגון המתנגד למשטר האייתוללות עוד מזמן המהפכה האסלאמית.

עוד הוסיף וקסלר, במהלך שבוע הסייבר של אוניברסיטת תל אביב כי "הפעם, נראה שמדובר במתקפה משמעותית יותר שהתמקדה במערכות לבקרה תעשייתית. מדובר במכונות תעשייתיות המחוברות למחשבים בשביל שליטה מרחוק. מתקפות אלו מחייבות היכרות טובה מאוד עם הארכיטקטורה של המפעל ולכן מחייבת יכולות מודיעיניות טובות - דבר שעשוי לרמוז דווקא על קשר מדינתי או על האקרים שמקבלים סיוע פנימי מצוות המפעלים.

"תקיפות מסוג זה יוחסו בעבר בעיקר למדינות ושירותי מודיעין זרים, אך קהילת המחקר הזהירה בשנה האחרונה שגם גורמים לא מדינתיים שמים את ידיהם על יכולות תקיפה מתקדמות שעשויות לאפשר תקיפות כאלה. בכל אופן, לאיראן יש אויבים רבים וקשה לקבוע בשלב זה מי באמת עומד מאחורי זה", סיכם המומחה.

לחברת הפלדה חוזסטן, שנמצאת באהווז שבמחוז חוזסטן העשיר במשאבים, יש מונופול על ייצור הפלדה באיראן יחד עם עוד שתי חברות בבעלות המדינה. החברה, שנוסדה בשנת *1979*, לפני המהפכה האסלאמית, פעלה באופן רציף מאז הקמתה, למעט במהלך מלחמת איראן-עיראק בשנות ה-80. איראן היא יצרנית הפלדה המובילה במזרח התיכון, ונמנית עם עשר היצרניות הגדולות בעולם. מכרות עופרת הברזל שלה מספקים חומרי גלם לעשרות מדינות, כולל איטליה, סין ואיחוד האמירויות.

"למרות לקיחת האחריות, קשה ומוקדם לדעת מטעם מי פועלת קבוצת ההאקרים", אמר עמרי וקסלר, חוקר בכיר במרכז הסייבר של אוניברסיטת תל אביב, באירועי שבוע הסייבר. "לא מן הנמנע כי מדובר בקבוצות אקטיביסטים או מתנגדי משטר שפועלות באיראן ומחוצה לה. תקיפות רבות, פחות משמעותיות, יוחסו בעבר גם לארגון מוג>הידין א-חלק, המתנגד למשטר האייתוללות עוד מזמן המהפכה האסלאמית.

"הפעם נראה שמדובר במתקפה משמעותית יותר שהתמקדה במערכות לבקרה תעשייתית. מדובר במכונות תעשייתיות המחוברות למחשבים לשם שליטה מרחוק. מתקפות אלה מחייבות היכרות טובה מאוד עם הארכיטקטורה של המפעל, כלומר מודיעין ברמה גבוהה - מה שעשוי לרמוז דווקא על קשר מדינתי או על האקרים שמקבלים סיוע פנימי מצוות המפעלי.

"תקיפות מסוג זה יוחסו בעבר בעיקר למדינות ולשירותי מודיעין זרים, אך קהילת המחקר הזהירה בשנה האחרונה שגם גורמים לא מדינתיים שמים את ידיהם על יכולות תקיפה מתקדמות שעשויות לאפשר תקיפות כאלה. בכל אופן, לאיראן יש אויבים רבים, וקשה לקבוע בשלב זה מי באמת עומד מאחורי המתקפה".

הארץ

חילופי המהלומות בין ישראל לאיראן נמשכים, בעיקר בתחום הסייבר - אך לא רק

בנט יוצא מהזירה ומשוכנע שהשאיר מורשת ביטחונית חמאס מציג אלטרנטיבות להתחממות ביטחונית, ויש לו סיבות לכך בבריטניה מסתכלים למוסקבה ונזכרים בברלין, של 1937 וכשהייצוא הביטחוני נוסק, עולות שאלות מוסריות

עמוס הראל

ההפחתה השבוע בחומרת אזהרת המסע לישראלים הנוסעים לאיסטנבול משקפת, לכל היותר, הקלה זמנית במתיחות הארוכה עם איראן. אחרי ששירותי הביטחון הטורקיים עצרו כמה חוליות שהתכוונו לחטוף או להרוג ישראלים, אפשר להוריד מעט את רמת הכוננות. אבל חילופי המהלומות בין הצדדים נמשכו גם השבוע, בעיקר בתחום הסייבר. בעוד שכישלון סדרת הפיגועים המתוכננת, וכעסם של הטורקים, הביכו את המשטר בטהראן ואילצו אותו כנראה לקחת צעד לאחור, בסייבר אין הפוגה לרגע. מראש, מרחב ההכחשה האיראני שם גדול יותר. תמיד אפשר לטעון שמדובר בעוד שקר ישראלי וטהראן אינה אחראית ליוזמות תקיפה של קבוצות האקרים עצמאיות, המוטרדות בכלל מהמשך הכיבוש בשטחים.

בפועל, היקף התקיפות האיראניות בסייבר גדל מאוד, ונראה שבאחרונה נרשמו הצלחות. זו מסתמנת כסיבה להגברת התקיפות על התשתית הדיגיטלית באיראן, שהעיתונות הבינלאומית מייחסת לישראל. השבוע הושבתה תשלובת של מפעלי פלדה גדולים כתוצאה מתקיפת סייבר. זה אחד הענפים הכלכליים הגדולים באיראן ונראה ששיקום הנזקים יארך שבועות אחדים.

ראש הממשלה היוצא, נפתלי בנט, ושר הביטחון, בני גנץ, התייחסו בעקיפין לאירועים בנאומים בכנס הסייבר באוניברסיטת תל אביב. בנט השווה באופן חריג הרתעה בסייבר להרתעה גרעינית והודיע: "אם מישהו תוקף אותנו בסייבר, אנחנו נתקוף בחזרה" — דברים שיכולים כמעט להתפרש כנטילת אחריות. גנץ טען: "אנחנו יודעים מי הטרוריסטים עם המקלדת, אנחנו פוגעים בהם ובשולחיהם וגם היום הם על הכוונת שלנו — ולא רק בממד הקיברנטי".

הטון החריף של הדברים מעיד שלא מדובר רק בהפרחת איומים על רקע מערכת הבחירות המתחדשת. נוצר הרושם שישראל ספגה מכות באחרונה, ואולי הגיבה בהתאם. התקריות המרובות, לסוגיהן השונים, ערערו מעט את הביטחון העצמי של המשטר בטהראן. העיתון ניו יורק טיימס דיווח שלשום כי בהנהגה האיראנית חשים שישראל חדרה לתוך ארגוני המודיעין ופועלת בתוך המדינה באין מפריע. זה, לצד הכישלון בטורקיה, כנראה הרקע לשורת הדחות וחילופי תפקידים בצמרת משמרות המהפכה. לפי העיתון, נעצר באחרונה גנרל בחשד לריגול לטובת ישראל. בכירים ישראלים טענו בשיחה עם "הארץ" כי המשבר הפנימי חמור, בעיקר בהנהגת המשמרות.

רגע לפני שהעביר את תפקיד ראש הממשלה ליאיר לפיד, יצא בנט ביום שלישי האחרון לסיבוב פרידה במטות המוסד ושב"כ. בנט חולק על הטענה, שהושמעה גם כאן, שלפיה מדיניותו הביטחונית אינה שונה מאוד משל קודמו, בנימין נתניהו — וההבדל ביניהם טמון בעיקר בסגנונו הממלכתי והמאופק. בעיניו, הוא הניח את היסודות לאסטרטגיה חדשה, הן באיראן והן מול הפלסטינים. כלפי איראן, הוביל קו לוחמני יותר, הכולל על־פי הדיווחים בחו"ל גם שימוש בנשק נגד מטרות שאינן קשורות בפרויקט הגרעין ונמצאות על אדמתה: השמדת בסיס ומפעל ייצור מל"טים בפברואר האחרון והתנקשות בחיי בכיר במשמרות המהפכה במאי. לאלה נוספו, כך דווח, תקיפות סייבר מרובות. נראה שהמטרה היא לבסס יכולת תגובה מהירה, כך שאיראן תשלם מחיר מיידי על כל פגיעה.

בנט מצא בארגוני המודיעין הקטנים מידה רבה יותר של גמישות מחשבתית ונכונות להשתנות מהירה, בהשוואה לצה"ל. הצבא הוא ספינה כבדה יותר וקשה לניווט. מה גם שהרמטכ"ל, אביב כוכבי, נכנס היום לחצי השנה האחרונה של כהונתו.

תרגיל בכלכלה

התרגיל שעשה חמאס השבוע לא זכה עד כה להצלחה. הארגון פרסם ביום שלישי סרטון קצר שבו נראה הישאם א־סייד, האזרח הישראלי המוחזק בניגוד לרצונו ברצועת עזה מאז 2015. זה היה אות החיים הראשון מא־סייד אחרי קרוב לשבע שנים. חמאס טוען שמצבו הבריאותי הידרדר. בסרטון הוא נראה שוכב במיטה כשמסכת חמצן על פניו. אביו, שעבאן, אמר בראיונות לתקשורת שלא הבחין בבעיה בריאותית מובהקת בסרטון.

בנט וגנץ האשימו את חמאס בניסיון לעשות מניפולציה על חשבונם של פגועי נפש (א־סייד והישראלי השני המוחזק בעזה, אברה מנגיסטו, סובלים מבעיות דומות). הם לא שידרו נכונות להתפשר במו"מ על עסקת חילופי אסירים. ייתכן שיחיא סינוואר, מנהיג חמאס ברצועה, אינו קורא נכון את תמונת המצב בישראל, למרות העברית המצוינת שלו ו–22 שנות המאסר שריצה בכלא בארץ.

בניגוד לעסקת שליט, אין כעת בישראל תנועה עממית נרחבת הדורשת מהממשלה ויתורים כבדים תמורת שחרורם של השניים והחזרת גופות שני החיילים, סרן הדר גולדין וסמל־ראשון אורון שאול. ספק אם גם פתיחת מערכת הבחירות תשפר את סיכויי חמאס לסחוט עסקה נדיבה יותר מממשלת המעבר. הפערים בין הצדדים גדולים, בעיקר משום שחמאס מתעקש שמאות המשוחררים יכללו גם אסירי עולם שנשפטו על רצח.

הארגון זקוק לעסקה על רקע מעמדם החשוב של האסירים הביטחוניים בקרב הציבור הפלסטיני וגם בשל הבטחה שלא נפרעה: כשסינוואר השתחרר מהכלא הישראלי בעסקת שליט ב–2011 הוא הבטיח לחבריו שנשארו מאחור כי יסייע לחלצם. עם זאת, מעניין שחמאס משתמש בתרגיל כזה בניסיון לקדם את המו"מ ואינו מחמם את הזירה הצבאית עצמה. גם לאורך ההסלמה האחרונה בפיגועים בגדה המערבית ובתחומי הקו הירוק, שהחלה במארס ודעכה חלקית במשך יוני, חמאס עודד במרץ טרור, אך דאג שלא להסלים את המצב בגבול הרצועה.

הקרב של בריטניה

יותר מארבעה חודשים אחרי שהחלה, המלחמה באוקראינה כמעט נשכחה מבחינתם של הציבור וכלי התקשורת בישראל. בשטח עצמו, הלחימה ניטשת בעוצמה, אולם ההתפתחויות האסטרטגיות מועטות. צבא רוסיה מגדיל את השטח שכבש באזור דונבאס, במזרח אוקראינה ואילו האוקראינים נחלו הצלחות בהדיפת הפולשים בצפון המדינה, בעיקר באזור הסמוך לבירה קייב. מספרי ההרוגים נאמדים בעשרות אלפים לכל צד, בהם קרוב ל–5,000 אזרחים אוקראינים. אוקראינה מחזיקה מעמד, תודות לרוח לחימה של אנשיה וסיוע מקיף, במודיעין ובנשק, מצד כמה מדינות במערב. אבל משטר פוטין משדר נכונות להמשיך במלחמת התשה ארוכה, בלי קשר למספר הנפגעים. המלחמה עלולה להתארך עמוק לתוך החורף הבא.

השבוע נאם הרמטכ"ל הבריטי, הגנרל סיר פטריק סנדרס, בכנס של מכון המחקר רוס"י בלונדון והציג מסקנות ביניים של צבא בריטניה על המלחמה. סנדרס בחר לצטט דברים שאמר הפילדמרשל ברנרד מונטגומרי, גיבור מלחמת העולם השנייה ב–1937, שנתיים לפני פרוץ המלחמה: "עלינו לפתח שיטות חדשות. אין צורך להמשיך לעשות אותו דבר רק כי הצבא עשה אותו ב–30 השנים האחרונות. אם זו הסיבה היחידה להמשיך לעשותו, הרי שהגיע הזמן לשנות".

המשמעות עבור הצבא הבריטי, אמר סנדרס, היא להכין את אנשיו לאיום חדש, סכנה ברורה ומיידית שהומחשה בפלישת רוסיה לאוקראינה בפברואר השנה. "בכל שנותיי במדים, לא ראיתי איום כה ברור לעקרונות הריבונות והדמוקרטיה כמו הברוטליות של הנשיא פוטין ושאיפות הסיפוח שלו", תיאר. "אנחנו חיים בתקופה משמעותית כמו זו שעברו קודמינו, לפני 80 שנה. זה רגע 1937 שלנו. איננו במלחמה, אבל עלינו לפעול במהירות כדי שלא ניגרר לתוכה בגלל כישלון במניעת סיפוח שטחים. אעשה כל שביכולתי כדי לוודא שהצבא הבריטי ממלא תפקיד במניעת מלחמה. תהיה לי תשובה לנכדיי כשישאלו אותי מה עשיתי ב–2022".

לפי סנדרס, הצבא בפיקודו עסוק כעת ביותר מדי משימות. נדרשים לו "תֶעדוף חסר רחמים" בין מטלותיו והתמקדות בעיקר. מעתה, תהיה לו מטרה ממוקדת אחת: "להתמודד עם האיום הנוכחי ולמנוע מלחמה באירופה". זה יחייב האצת תהליכי הצטיידות והטמעת טכנולוגיה, שיפור המוכנות של היחידות ללחימה ושינויים מבניים בצבא.

בתוך כך, הורחב מאוד הסיוע לאוקראינה: הבריטים אימנו בזמן המלחמה מאות חיילים אוקראינים וסיפקו להם אלפי טילי נ"ט. לדבריו, "מסוכן להניח שאוקראינה היא סכסוך מוגבל. אחד הלקחים הוא שפוטין לא תמיד מתנהל בהתאם להגיון שלנו". לעתים קרובות, הוסיף, רוסיה מתחילה רע את מלחמותיה, אבל עומק היכולות שלה, נחישותה ונכונותה לסבול מאפשרים לה לסיים בהצלחה. סנדרס סבור שנאט"ו צריכה להפגין קו נוקשה יותר כדי להרתיע את רוסיה. על מוסקבה לדעת שכל מתקפה שלה תיענה בתגובה צבאית מיידית — ולא בסיוע מאוחר שתגיש הברית לצד המותקף, אחרי שהרוסים כבר קבעו עובדות בשטח.

הרמטכ"ל הבריטי מנה בנאומו עוד שינויים רבים ונרחבים שנדרשים לדעתו בצבאו. בעיניים ישראליות יש כאן שני דברים בולטים. ראשית, הבריטים אינם חוששים להפיק לקחים ממה שמתרחש באוקראינה ולהגיב במהירות להתפתחויות. ושנית, בניגוד לישראל המתחמקת מכך כבר כמה חודשים, הם אינם נרתעים מנקיטת עמדה מוסרית ברורה נגד התוקפנות הרוסית.

לעיני הינשו"ף

המלחמה באוקראינה מביאה עמה גם תקוות לבוננזה כלכלית לתעשיות הביטחוניות, בישראל ובמדינות אחרות. לא רק שכנותיה החרדות של רוסיה מצטיידות בנשק, גם דמוקרטיות במערב אירופה ובמזרח אסיה שתקציב הביטחון שלהן הלך והצטמצם מאז התמוטטות הגוש הסובייטי וכעת מתרחב מחדש. גנץ הנחה באחרונה את מנכ"ל משרדו, אלוף במילואים אמיר אשל, לבדוק כיצד ניתן להאיץ הליכי ייצור למקסימום, כדי שישראל תוכל להגדיל את הייצוא הביטחוני שלה בנסיבות החדשות.

הרב אבידן פרידמן הוא מנכ"ל ארגון בשם ינשו"ף (ראשי תיבות של יצוא נשק, שקיפות ופיקוח). פרידמן, שעלה לארץ מקנדה, מתגורר בהתנחלות אפרת בגוש עציון ומלמד בתיכון הרטמן בירושלים — אולי לא בדיוק הפרופיל הצפוי של הישראלי שייצא למאבק ציבורי למניעת אספקת נשק למשטרים מפוקפקים. בשיחה עם "הארץ" הוא אומר כי הושפע עמוקות מהרצאה ששמע מפי פעיל אחר באותו תחום, אלי יוסף, לפני כחמש שנים למורי התיכון.

"הייתי המום, לא היה לי מושג שזה קורה. איכשהו החינוך הציוני שלי דילג על התופעות הללו", סיפר. "אלי היה הראשון ששם לי את זה מול הפרצוף — את הטענות שנשק שיוצר בישראל משמש לרצח עם, לטיהורים אתניים. והוא עוד אדם שבא מהצד הימני של המפה. היה קשה לדחות את הדברים שלו בהינף יד".

פרידמן עמד בקשר עם עו"ד איתי מק, שהגיש שורת עתירות נגד משרד הביטחון בשל מכירות נשק למשטרים בעייתיים. ב–2017 הסלים העימות הפנימי במיאנמר (בורמה) שבדרום מזרח אסיה. ארגוני זכויות אדם הזהירו שצפוי שם טבח המוני. מק עתר לבג"ץ בדרישה להפסיק מכירת נשק ישראלי למשטר הרודני במדינה. משרד הביטחון ביקש חיסיון, למרות פרסומים ב"הארץ" ובעמוד הפייסבוק הרשמי של צבא מיאנמר, שלפיהם הרמטכ"ל הבורמזי ביקר בישראל ובחן מערכות נשק שונות.

בחורף 2018 הפסיקה ישראל את מכירות הנשק, אבל בזמן שחלף עד אז כבר אירעו מעשי אלימות קשים. עשרות אלפי אזרחים נהרגו ומאות אלפים נהפכו לפליטים. הצטברו עדויות ברורות למעשי זוועה ובהן צילומי לוויין של כפרים שנשרפו כליל. לפי פרידמן, המקרה הזה אינו ייחודי. "ישראל מוכרת לכל מיני מדינות. אני יכול להבין שיש אינטרס של המדינה לייצא נשק לאזרבייג>אן, למרות אופי המשטר שם, כשהיא שוכנת בגבולה הצפוני של איראן. אבל מה האינטרס שלנו במיאנמר? מה הצדיק אספקת נשק למשטר רצחני? כאזרח אין לי שום דרך ליישב את הסתירה בין הסיוע למיאנמר לשיקולים מוסריים. אני לא יכול לדמיין לעצמי מה מצדיק להמשיך ולמכור להם נשק ישראלי, כמה חודשים לפני שמתחילים מעשי הטבח.

"הטענה הקבועה של המדינה היא שאינה מוכרת נשק לדיקטטורות. בפועל, יש כל מיני תרגילים שבאמצעותם הנשק מגיע דרך מדינות מתווכות. אין רשימה מלאה של עסקאות הנשק בחו"ל וכך קל למדינה להכחיש ולנו קשה לפקח. אנחנו אוספים מידע מפרסומים בתקשורת הזרה, מעתירות משפטיות, מדו"חות של ארגוני זכויות אדם, אבל אין לנו תמונה מלאה. מה שמתפרסם הוא קצה הקרחון. בחודשים האחרונים היו מעשי זוועה במלחמה באתיופיה. פורסם שישראל מכרה נשק לצבא אתיופיה, דרך אוגנדה. ישראל התחייבה לקבוע גבולות מוסריים ורמת שקיפות כנהוג במדינות העולם המערבי. צריך ליישם את זה — לתת מעמד מכריע לשיקולים אתיים ולחזק את הפיקוח הביטחוני על העסקאות".

"מה הצדיק אספקת נשק למשטר רצחני? כאזרח אין לי שום דרך ליישב את הסתירה בין הסיוע למיאנמר לשיקולים מוסריים"

הרב אבידן פרידמן

מקורות ביטחוניים טוענים, לעומת זאת, שהפיקוח על הייצוא הודק מאוד בשנים האחרונות. הם הזכירו, בין השאר, את צמצום רשימת המדינות שלהן ניתן למכור טכנולוגיית סייבר התקפי, אחרי התפוצצות פרשת אן־אס־או בתחילת השנה. ב–2007 הוקם אגף הפיקוח על הייצוא במשרד הביטחון, בעיקר עקב חיכוכים בין ישראל לארצות הברית סביב עסקאות נשק בין ישראל להודו ולסין. "מדי פעם פוסלים עסקאות מכירה קטנות לדיקטטורות אפריקאיות", אומר פרידמן. "אבל אני לא מוכן להשלים עם המצב הקיים. זה עושה אותי שותף באחריות למעשים הללו, כאזרח ישראלי. אנחנו שותפים באשמה ובאחריות למעשים. מה גם שצעירים משתחררים מיחידות עילית והולכים לאמן כוחות במדינות בעייתיות. זו שחיתות מוסרית, שחוזרת אלינו בכל מיני דרכים".

מקור ראשון

עד היום זכתה הפעילות של ינשו"ף ופעילים אחרים לקשב תקשורתי מועט. זה לא פוגם באופטימיות של פרידמן. "אני משוכנע שאפשר לשנות", הוא אומר. "רוב אזרחי ישראל לא מודעים לכך, אבל הם יתמכו בפיקוח הדוק יותר אם הגישה תוצג להם. המטרה שלנו היא להביא את העניין הזה למודעות. כבר מצאנו אוזן קשבת אצל כמה ח"כים מימין ומשמאל".

ב–2021 קפץ ייצוא הנשק הישראלי לשיא של כל הזמנים — 11.3 מיליארד דולר, עלייה עצומה בהשוואה ל–7 מיליארד דולר בשנה הקודמת. "הדמוקרטיות הן יותר מ–60% מהמדינות שקונות את הנשק הישראלי. אף שיש הסתייגויות מהנעשה בהודו, אין אמברגו נשק על הודו ולא יהיה. אינני תמים", אומר פרידמן. "אבל הפוליטיקאים צריכים להגיד באופן ברור שחייבים להתחשב בשיקולים מוסריים כשחותמים עסקאות נשק. זה יקרה רק אם נצליח לגייס לחץ ציבורי. אין לי בעיה אם נמכור יותר נשק למדינות כמו בריטניה ושווייץ. אבל כלכלת המדינה לא תיפול אם נבטל עסקה בעייתית עם דיקטטורה בעולם השלישי".

סגן מפקד יחידת 8200 חושף: "סיכלנו ניסיונות להשתלט על מערכות המים"

אורי, סגן מפקד יחידת 8200 בהופעה ציבורית נדירה סיפר על המאמצים של היחידה לסכל פיגועים שנוגעים גם לחברות אזרחיות

נועם אמיר

יחידת 8200 של צה"ל היא זו שסכלה את הניסיון של איראן להשתלט על מערכות המים המרכזיות של ישראל במטרה להרעיל את המים. אורי, סגן מפקד יחידת 8200, חשף הבוקר את הדברים בהופעה נדירה של סגן מפקד היחידה בשבוע הסייבר השנתי בהובלת המרכז למחקר סייבר באוניברסיטת ת"א. "זוהי ההופעה הפומבית הרשמית הראשונה של 8200" ציין הקצין. "זאת למרות שמזה כבר כמה עשרות שנים אנחנו מהווים חלק ניכר ממערך ההגנה והמודיעין של ישראל והמשימה שלנו היא איסוף מודיעין על איומים מכריעים על ישראל. ידוע לכל שאנחנו מהווים שחקן מרכזי בתחום הסייבר בישראל ומעבדים את המידע באמצעות כלים שפותחו אצלנו. המידע שאנו מקבלים מגיע ממקורות שונים משותפים".

עוד הוסיף הקצין "אנחנו סיכלנו את הניסיון להשתלט על מערכות המים הקריטיות של ישראל ולהרעיל אותן לפני מספר שנים. במקרה אחר זיהינו גם כי יריב מסוים תקף את ישראל ותוך כדי זיהינו שאותו תוקף ניסה גם לכוון לתחנות כוח בארה"ב. זו הייתה האינדיקציה הראשונה להתקפה זו. את האיום הזה הצלחנו למנוע באמצעות שיתוף פעולה הדוק עם השותפים האמריקאים שלנו. הישגים כאלו הם שגורמים לחיילים שלנו להיות גאים בעבודתם ב-8200".

מערכת הביטחון בעיקר עוסקת בהגנה על מערכות ביטחוניות ומתקנים אסטרטגים אולם בשנים האחרונות המוחות של היחידה פעלו לא מעט במרחב האזרחי כדי לסייע במניעת תקיפות בעיקר על רקע לאומני או כאלו שהנזק לחברות היה משפיע בצורה דרמטית על המדינה. גם סגן מפקד היחידה מודה שהאחריות בסוף במדינה כל כך קטנה שהצבא הוא חלק מהעם ש-8200 תמיד יהיו מוכנים לעזור.

"רוב מה שאנחנו עושים הוא חסוי ואנחנו פועלים על מנת למנוע איומי סייבר נגד ישראל ומבטיחים שישראל תישאר מעצמה מובילה בתחום הטכנולוגיה והסייבר באזורנו. בתוך המרחב הזה יש לנו אחריות על אתיקה, מוסר וערכים ואנו לוקחים אותה ברצינות רבה, תוך שמירת מחויבות לערכים הדמוקרטיים שלנו, לנורמות במרחב הסייבר, ולחברה הישראלית וזו הסיבה העיקרית שאני עומד פה היום".

עוד הוסיף הקצין "האחריות שיש לנו כלפי החברה הישראלית ואנחנו יודעים שלגיוון בגיוסים שלנו יש השפעה אחר כך על הגיוון בהייטק הישראלי. לצד יחידות נוספות בצה"ל הרחבנו בשנה שעברה את תכנית <גשרים> מתיכונים לחטיבות הביניים ובשנה הבאה נרחיב את התכנית ליותר מ-20 רשויות נוספות ואנחנו צופים השתתפות של יותר מ-20 אלף בני נוער. בעשור האחרון, קלטנו צעירים רבים גם מהפריפריה ואני בטוח שזה ישפיע על התעשייה והחברה גם בעשור הקרוב".

מעריב

שבוע הסייבר הישראלי

קבוצת Team8 שבונה ומשקיעה בחברות סייבר ופינטק ערכה בראשון אירוע ענק לפתיחת שבוע הסייבר הישראלי. האירוע התקיים בשיתוף עם; Deloitte, לאומי-טק, משרד עו"ד מיתר, Valley Bank, פאלו אלטו ו- FinSec מעבדת החדשנות של Mastercard ו-Enel. את האירוע הנחתה השחקנית, ניב סולטן הידועה בתפקידה כהאקרית סייבר בסדרה "טהרן" שהזכירה לכולם שהיא זאת שפרצה לכור הגרעיני ואפילו אמרה כמה מילים בפרסית, היא התרגשה לפגוש את רנה ווין, בכירה מנאס"א ואמרה לה שהיא השראה אמיתית לנשים.

בין הדוברים באירוע באירוע ניתן למנות את נדב צפריר, מפקד יחידת 8200 לשעבר ושותף מנהל בקבוצת Team8, מייק רוג'רס ראש ה- NSA לשעבר ושותף ב-Team8 וניר מינרבי מנכ"ל ומייסד סטארטאפ המחשוב הקוונטי, Classiq. כמו כן, באירוע נכחו ברק רגב, מנכ"ל גוגל ישראל; שגריר ישראל בארה"ב לשעבר דיוויד פרידמן; מיכל גבע, מייסדת טרייונצ>רס; שותפים בTeam8: רקפת רוסק עמינח, שרית פירן, יובל טל, לירן גרינברג ועוד.

ice.

מה הביא את ניב סולטן לכנס הסייבר הישראלי?

כנס הסייבר הישראלי יצא לדרך השבוע ובאירוע השקה חגיגי הגיעה רשימה מכובדת של סלבס לצד בכירים מעולם הביטחון מכל העולם

שבוע הסייבר הישראלי הוא אירוע שיא שנתי שמתקיים זו השנה ה- 12 במרכז הסייבר ע"ש בלווטניק באוניברסיטת תל אביב ובשיתוף מערך הסייבר הלאומי. הכנס מפגיש מדי שנה בין מומחי סייבר וחוקרים מובילים מהארץ ומהעולם, לצד קובעי מדיניות, אנשי ביטחון מהארץ ומהעולם, דיפלומטים וראשי תאגידים בינלאומיים בתחום לסבב שולחנות עגולים, הרצאות, דיונים וסדנאות ועוד.

לאור זאת, חברת התוכנה ומיזם הסייבר הישראלי Team 8 ערכה אתמול (יום ב>) אירוע חגיגי לכבוד פתיחת שבוע הסייבר הישראלי. את האירוע נערך באולם האירועים "טראסק" והנחתה אותו השחקנית ניב סולטן. בהמשך הערב עלו לבמה מספר כוכבים, ביניהם: מארינה מקסימיליאן בלומין ורד בנד. כמו כן, באירוע נכחו בכירים מסוכנות החלל האמריקאית NASA ומהסוכנות לביטחון לאומי NSA.

כלכליסט

"הדה-גלובליזציה וההאטה הכלכלית בעולם מגבירים את סיכוני הסייבר"

כינוס פסגה של תעשיית הסייבר העולמית יתקיים השבוע בישראל בהשתתפות 100 מנהלי אבטחת המידע בחברות המובילות בעולם. נדב צפריר, שותף מנהל בקבוצת Team8, שיזמה את האירוע: "נדון ביחד בהזדמנויות ובאתגרים הניצבים בפנינו וכיצד על החברות להיערך להחרפת סיכוני הסייבר"

על רקע השינויים הכלכליים והגאופוליטיים בעולם, יוצא היום לדרך פורום ה-CISO העולמי, בהובלת קבוצת Team8. בפורום, המכנס את פסגת תעשיית הסייבר, ייקחו חלק למעלה מ-100 מנהלי אבטחת מידע בכירים בחברות המובילות בעולם, ובהן Walmart ,Uniliver GM Financial, Intuit, Mastercard ועוד.

במסגרת הפורום ידונו הבכירים בעתיד אבטחת הסייבר בדגש על אתגרים והזדמנויות גלובליים, השפעתם של השינויים הכלכליים והגיאופוליטיים על תעשיית הסייבר בתחומים שונים כגון אבטחת ענן, IT ,OT, 5G, פרטיות, רגולציה והשינוי החל באסטרטגיות התקיפה והתוקפים. מנהלי האבטחה ייפגשו עם שורת יזמים, משקיעים ואנשי עסקים בולטים בתעשיית ההייטק הישראלית, ובסיום ייקחו חלק באירוע פתיחת שבוע הסייבר הישראלי.

דיוני הפורום יימשכו חמישה ימים, ויכללו דיונים על אתגרי התקופה ופתרונות מותאמים לתקופה, וכן על אודות חשיבותו הגוברת של תפקיד ה-CISO והשפעתו על האסטרטגיה העסקית של הארגון. במהלך ביקורם בארץ ייפגשו עם סטארט-אפים ישראליים מובילים, ובהם Claroty, Sygnia, Talon, Akeyless, Illusive, Cyberpion, Silverfort, Authomize, Cardinal, Orca Security, Ermetic, Safebreach, Resilion במטרה לחשוף אותם לטכנולוגיות ישראליות.

נדב צפריר, שותף מנהל בקבוצת Team8: "בשבועות האחרונים אנו עדים לשינויים משמעותיים המתאפיינים בדה-גלובליזציה והאטה כלכלית, המשפיעים באופן דרמטי על העולם ועשויים גם להשפיע באופן ישיר על תדירות מתקפות הסייבר והפיכתו לכלי משמעותי מאי פעם. אנחנו ב-Team8 זיהינו צורך אמיתי בכינוס טובי מומחי הסייבר בעולם, ובהם כמאה CISOs מהחברות המובילות יחד עם מובילי הדעה בתעשייה הישראלית, במטרה להבין יחד מהם האתגרים וההזדמנויות הניצבים בפנינו וכיצד עלינו להיערך בהתאם".

מעריב

כינוס פסגה של תעשיית הסייבר העולמית יתקיים בישראל

על רקע השינויים הכלכליים והגיאופוליטיים בעולם יוצא לדרך פורום ה-CISO העולמי בהובלת קבוצת Team8, וישתתפו בו למעלה מ-100 מנהלי אבטחת מידע

על רקע השינויים הכלכליים והגיאופוליטיים בעולם, היום (רביעי), יוצא לדרך פורום ה-CISO העולמי בהובלת קבוצת Team8. בפורום המכנס את פסגת תעשיית הסייבר, ייקחו חלק למעלה מ-100 מנהלי אבטחת מידע בכירים בחברות המובילות בעולם בניהם: Walmart, Uniliver, GM Financial, Intuit, Mastercard ועוד.

במסגרת הפורום ידונו הבכירים בעתיד אבטחת הסייבר בדגש על אתגרים והזדמנויות גלובליים, השפעתם של השינויים הכלכליים והגיאופוליטיים על תעשיית הסייבר בתחומים שונים כגון אבטחת ענן, IT ,OT, 5G, פרטיות, רגולציה והשינוי החל באסטרטגיות התקיפה והתוקפים. מנהלי האבטחה ייפגשו עם שורת יזמים, משקיעים ואנשי עסקים בולטים בתעשיית ההייטק הישראלית ובסיום ייקחו חלק באירוע פתיחת שבוע הסייבר הישראלי.

דיוני הפורום יחלו ביום רביעי, 22.06 למשך חמישה ימים, ויכללו דיוני עומק על אתגרי התקופה ופתרונות מותאמים לתקופה, וכן אודות חשיבותו הגוברת של תפקיד ה-CISO והשפעתם על האסטרטגיה העסקית של הארגון. במהלך ביקורם בארץ ייפגשו עם סטארטפים ישראליים מובילים ובינהם: Claroty, Sygnia, Talon, Akeyless, Illusive, Cyberpion, Silverfort, Authomize, Cardinal, Orca Security, Ermetic, Safebreach, Resilion במטרה לחשוף אותם לטכנולוגיות ישראליות. בנוסף, הם ישתתפו בארוחות ערב וקבלות פנים עם יזמים, משקיעים ואנשי עסקים בולטים בתעשיית ההייטק הישראלית באירוח של ארגונים שונים בתעשייה.

פורום ה-CISO Village של קבוצת Team8 מהווה נדבך חשוב במודל הייחודי של הקבוצה לבניית חברות, והוא משמעותי בתהליך הרעיונות והמחקר אחר פתרונות טכנולוגיים של החברות, מסייע בהתאמת המוצרים לשוק ותורם רבות לצמיחה חברות הפורטפוליו של Team8. בבסיס ה-Village עומד הרציונאל ששיתוף הפעולה עם החברות המובילות בעולם יניב הזדמנויות עסקיות לכל הצדדים ויסייע בזיהוי הבעיות והצרכים האמיתיים של הארגונים הגדולים, להן יספקו מענה טכנולוגי החברות שיוקמו לצורך יצירת פתרונות אלו.

סיומו של כינוס זה ישתלב עם אירוע הפתיחה הרשמי של שבוע הסייבר בישראל של אוניברסיטת ת"א, שיתקיים בין התאריכים 27-30 ליוני. את האירוע תארח Team8 יחד עם שותפים נוספים מהתעשייה; Deloitte, לאומי-טק, משרד עו"ד מיתר, Valley Bank, פאלו אלטו ו- FinSec מעבדת החדשנות של Mastercard ו-Enel.בין הדוברים באירוע ניתן למנות את רנה ווין, מנהלת האבטחה לשעבר בנאס"א, מייק רוג'רס ראש ה- NSA לשעבר ושותף ב-Team8, נדב צפריר, מפקד יחידת 8200 לשעבר ושותף מנהל בקבוצת Team8, וניר מינרבי מנכ"ל ומייסד סטארטאפ המחשוב הקוונטי, Classiq. את האירוע תנחה השחקנית, ניב סולטן הידועה בתפקידה כהאקרית סייבר בסדרה טהרן.נדב צפריר, שותף מנהל בקבוצת Team8: "בשבועות האחרונים אנו עדים לשינויים משמעותיים המתאפיינים בדה גלובליזציה והאטה כלכלית, המשפיעים באופן דרמטי על העולם ועשויים גם להשפיע באופן ישיר על תדירות מתקפות הסייבר והפיכתו לכלי משמעותי מאי פעם. אנחנו ב-Team8 זיהנו צורך אמיתי בכינוס טובי מומחי הסייבר בעולם ובינהם כמאה CISOs מהחברות המובילות יחד עם מובילי הדעה בתעשייה הישראלית לחמישה ימים מלאים של דיוני עומק במטרה להבין יחד מהם האתגרים וההזדמנויות הניצבים בפנינו וכיצד עלינו להערך בהתאם".

Cyber Week

June 27th-30th, 2022

Tel Aviv University, Israel

Yuval Ne'eman Workshop for Science, Technology and Security Tel Aviv University

Blavatnik Interdisciplinary Cyber Research Center

TEL AVIV UNIVERSITY אוניברסיטת תל אביב

Cyber Israel National Cyber Directorate

In cooperation with:

Ministry of Foreign Affairs Israel

ISRAEL CYBER ALLIANCE

State of Israel Ministry of Economy and Industry Foreign Trade Administration

ISRAEL EXPORT INSTITUTE

עליית מחירי הכופרה - ראיון עם מני ברזילי

העתיד עכשיו: סיקור שבוע הסייבר וראיונות עם משתתפים