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 26th-29th, 2023

Tel Aviv University, Israel

Press Kit

PUBLIC RELATIONS (INTERNATIONAL): STRAUSS PR

Cyber Week

June 26th-29th, 2023

Tel Aviv University, Israel

Press Kit

SPONSORS & PARTNERS

Distinguished Benefactor

THE SAGOL NETWORK

Distinguished Partner

DDR&D

MINISTRY OF DEFENSE

Diamond Sponsors

Google Cloud

Esteemed Platinum Sponsors

CHECK POINT

deep instinct

IAI Where Courage Meets Technology

PENTERA

YL VENTURES

Platinum Sponsors

ARMIS

CROWDSTRIKE

CYBERARK

Microsoft

SECURITY JOES

TEAM8

TREND MICRO

XM Cyber

Gold Sponsors

CLOUDFLARE

>_Code blue

cyberbit

Laminar

NOMINET CYBER

OPSWAT

RESCANA

SYNOPSYS

Silver Sponsors

Akamai

CLAROTY

CLASSIQ

CYLUS

CYVIATION

elastic

FinSec Innovation Lab

Mastercard

AYR

NASCHITZ BRANDES AMIR

Fox Rothschild LLP

intel capital

Porsche Digital Israel

MAZEBOLT

SAMSUNG NEXT

NTT Innovation Laboratory Israel

RAFAEL ADVANCED DEFENSE SYSTEMS LTD.

THETARAY

Trellix

Bronze Sponsors

BioCatch

T

FORTER

imperva

REUTERS

Israel’s Shin Bet spy service uses generative AI to thwart threats

Writing by Dan Williams; Editing by Conor Humphries

Israel’s Shin Bet security service has incorporated artificial intelligence into its tradecraft and used the technology to foil substantial threats, its director said on Tuesday, highlighting generative AI’s potential for law-enforcement.

Among measures taken by the Shin Bet - the Israeli counterpart of the U.S. Federal Bureau of Investigations or Britain’s MI5 - has been the creation of its own generative AI platform, akin to ChatGPT or Bard, director Ronen Bar said.

“AI technology has been incorporated quite naturally into the Shin Bet’s interdiction machine,” Bar said in a speech to the Cyber Week conference hosted by Tel Aviv University. “Using AI, we have spotted a not-inconsequential number of threats.”

AI has helped streamline Shin Bet work by flagging anomalies in surveillance data and sorting through “endless” intelligence, he said, adding that the technology also had a secondary role in decision-making “like a partner at the table, a co-pilot”.

Acknowledging the public-domain backbone of the fast-emerging technology, Bar urged cooperation between commercial hi-tech and government agencies such as his “to ensure AI leads to evolution and not to revolution”.

With Israel still pondering its AI policies, Bar called for the expected regulations to include a review of Shin Bet-related laws as well as a redefinition of official secrecy.

Israel is considered a world-leader in AI, thanks to burgeoning computing and robotics industries that draw on talent developed in the technologically-advanced conscript military.

FOX NEWS channel

Israel embraces cutting-edge AI to thwart cyberattacks, foil terrorism

Israel has found itself at forefront of AI capabilities for law enforcement, military

By Peter Aitken , Yonat Friling

Israel continues to explore innovative uses for artificial intelligence (AI) in various aspects of security and law enforcement, helping to foil numerous threats.

“AI technology has been incorporated quite naturally into the Shin Bet’s interdiction machine,” Shin Bet Director Ronen Bar said in a speech to the Cyber Week conference in Israel. “Using AI, we have spotted a not-inconsequential number of threats.”

Shin Bet, the Israeli counterpart to the FBI or Britain’s MI5, has created its own generative AI platform, akin to ChatGPT, Bar revealed. He explained that the platform has allowed the intelligence service to streamline its work by flagging surveillance anomalies and sort “endless” amounts of intelligence.

“Since the beginning of 2022, ISA handled 600 ISIS-related cases, many of them consumed similar violent and dangerous content on social media and on the web. Some were even arrested just before attacking,” Bar said. “They are added to roughly 800 major attacks we have foiled since January 2022.”

“An alarming number of them have a strong basis on the web – posts, inspiration, knowledge or social groups,” he added. “The trend is clear. Traditional security organizations must adapt to the new situation, where any angry person with access to the Internet may become a threat.”

“Already today, with AI, we have identified a significant number of threats,” he said. “The machine and its ability to detect anomalies create a protective wall against our enemies, alongside our traditional capabilities. ... Since we have understood we can’t fight this war with sticks and stones, we recognize the threats but also see

THE JERUSALEM POST

opportunities using AI."

Retired Maj. Gen. Isaac Ben-Israel, director of Blavatnik Interdisciplinary Cyber Research Center at Tel Aviv University, argued that the "accelerated increase in the use of artificial intelligence has a drastic impact on the cybersecurity arena, cyberdefense and the nature of malicious cyberattacks."

"Accelerating rise in the use of artificial intelligence has a drastic impact on the cybersecurity arena, cyberdefense and the nature of malicious cyberattacks," he said. "As the use of AI increases, our society becomes more and more dependent on computers, leading to a greater need for strong cyberdefense measures."

Gaby Portnoy, director-general of Israel National Cyber Directorate, told the Cyber Week conference that "Anyone who carries out cyberattacks against Israeli citizens must take into account the price he will pay."

"In the past year, we have been working hard to develop our resilience and expand our capabilities to detect cyberattacks, raise our shields and expose malicious activities, specifically Iranian," Portnoy said, adding that the vast majority of attacks are thwarted.

Portnoy described some of the projects the Cyber Directorate has pursued over the past year, saying that Israel is working with "our partner from the UAE [United Arab Emirates], His Excellency Dr. [Mohamed] Al Kuwaiti" to build "a multinational cybercollaboration platform for cyberinvestigation and knowledge building."

Rafael Advanced Defense Systems Ltd., a global leader in defense technology, helped develop a new system called Puzzle, which uses AI to combine and analyze visual data, communications information and other information to create a "comprehensive and filtered dataset," according to a company press release.

Puzzle seamlessly interfaces with existing command and control systems, helping to make sense of the incoming data to prioritize necessary targets within tight time frames, helping improve the efficacy of AI targeting.

Essentially, the Puzzle system works like a filter for the incredible amount of information AI can handle as many analysts and officials look to keep the human element involved in any AI-powered process.

Israel has remained on the cutting edge of AI and its uses across various security fields: The Israel Defense Forces (IDF) has invested in AI, which officials have argued presents "a leap forward" even as researchers raise concerns about the potential escalation it would create.

Col. Uri, head of the data and AI department, Digital Transformation Division, previously told Fox News Digital that "Anyone who wants to make such a change faces a huge challenge."

The IDF used AI in a 2021 operation to successfully target at least two Hamas commanders, producing "200 new target assets" by using the new digital methods to create likely targets and locations to hit.

"Because we don't have a lot of manpower, we need to find creative ways to compensate," Ram Ben Tzion, founder and CEO of tech firm Ultra, previously told Fox News Digital. "So, when it comes to data and intelligence, many times we've had to rely on innovation and technology to compensate for lack of resources, human or other."

Israel helped UAE fend off major cyberattack, Emirati cyber chief says

Israel's cyber chief called on top international cyber officials to work together to stop Iranian and Hezbollah hackers "from their attacks on the world."

By YONAH JEREMY BOB

Israel recently helped the UAE fend off a serious DDoS (distributed denial of service) cyberattack, UAE cyber chief Muhammad al-Kuwaiti said on Tuesday.

Speaking at the Tel Aviv Cyber Week Conference, he said, "Thank God for the Abraham Accords... Cybersecurity is an important aspect for us all. We in the UAE for example are going through a great digital transformation. A transformation across all sectors: aviation, education, healthcare, oil and gas, transportation. And, in fact, we need to do a safe and secure transformation."

Continuing he said, "I am sure you heard my dear friend, Gabi [Israeli cyber chief Gabi Portnoy], when he mentioned the importance of working together. Our cyber strategy has five main pillars," one of which is partnerships with allied states.

"It has a pillar about protecting and defending. And this is where we plug into the great Start-Up Nation [Israel] where we have many of those companies helping us as a matter of fact to build up that cyber dome or to extend that cyber dome," to defend against cyberattacks.

Israel's cyber chief uses generative AI to thwart threats

Earlier at the same conference, Israel National Cyber Directorate (INCD) chief Portnoy said, "anyone who carries out a cyberattack against Israeli citizens needs to take into account the price he will pay."

Portnoy specifically called out Iran and Hezbollah in his threat.

More specifically, he addressed cyberattacks by the group MuddyWater, which he identified as associated with the Islamic Revolutionary Guard Corps and which attacked the Technion-Israel Institute of Technology a few months ago.

"The group doesn't just work against Israel, but rather also hacks civilian targets in many other countries, including: Turkey, Saudi Arabia, Egypt, Morocco, India, Bahrain, Oman, Kuwait and others," said Portnoy.

This statement of Iran's attacks on Sunni states came despite the Islamic Republic's nominal improved relations with the Saudis and other Sunni states.

The INCD chief stated that in the past year, MuddyWater had tried to attack other targets in Israel, but unsuccessfully.

The people behind the attacks

He added, "The Israeli cyber community knows Iran's cyber operations inside-out and works to thwart it in many ways. Iran's intelligence personnel, the IRGC and Hezbollah who are involved in cyber operations against Israel know exactly what I am talking about."

Next, he said, "I want to back the actions of the US against Iran's violence, as well as the sanctions which they placed on two key players in Iranian intelligence: Farazin Karimi and Majteba Matzafi, who set up the Radwan Academic Group, which trains hackers for bad purposes."

Further, he flagged Ali Hidari who operates out of Beirut, and "who coordinates cyber operations between Iran and Hezbollah, which causes harm to the Lebanese civilian sector in the cyber area."

In addition, he said that for some in Iranian intelligence, using the digital sphere to harm civilians "is part of their routine."

Portnoy called on top international cyber officials to work together to stop Iranian and Hezbollah hackers "from their attacks on the world."

Separately, Portnoy praised Google, Microsoft and other private sector companies for helping Israel build its "cyber dome" – a digital Iron Dome against cyberattacks as well as for assisting in building a 40-country apparatus for investigating and sharing information relating to enemy cyberattacks.

THE JERUSALEM POST

AI rapidly changing cyberattack landscape, making collaboration crucial

With the advancement of artificial intelligence, both attackers and defenders are finding new ways to exploit and defend, making international collaboration on cybersecurity crucial

By DEBBIE MOHNBLATT/THE MEDIA LINE, HANNAH LEVIN

In the digital era, the cyber arena faces financially motivated attacks, increased state-sponsored threats, and new challenges posed by artificial intelligence, making international cyberdefense collaboration crucial.

Representatives from 25 countries gathered at Tel Aviv University on Monday for Cyber Week, a global cybersecurity event that brings together experts, industry leaders, investors, academics, and government officials.

"We must collaborate with like-minded states, share information, and cooperate to mitigate this risk," Dadi Gertler, executive director of innovation and technology partnerships at the Israel National Cyber Directorate, told The Media Line. "We all have the same goal and face the same challenges. The next step is to enhance collaboration between governments." According to Gertler, the presence of delegates from so many countries at Cyber Weekdemonstrates the existing demand for better international cooperation.

Cyberattacks have two chief causes: financial and political gain

Wafa Nimri, general manager of Levant and head of Arabic marketing at the UK-based Protection Group International, said many countries face similar threats. "All nations are encountering similar threats in cybercrime, misinformation, disinformation, and ransomware, which affect the supply chain," she told The Media Line. Nir Yaniv, chief business development officer & cyber operations at Code Blue, an Israeli company, told The Media Line that cyberattacks have two chief causes: financial and political gain.

Yaniv said state-sponsored attacks threaten both the private sector and government agencies. Sometimes, smaller private companies are more accessible to attack than government bureaucracies, which can benefit from more robust protections. "If the state mounts a strong defense, it's easier to attack private companies, create economicchaos, disturb markets, and hurt people," Yaniv said.

David Polton, vice president of Global Sales at Nominet, a UK-based cybersecurity company, told The Media Line that his group had seen a marked increase in state-sponsored cyberattacks over the last few years.

"Certainly, with a lot of the international warfare that we're seeing, I think you see a lot of change in how nations are targeting other nations, and the particular means they're using to do so are certainly getting more sophisticated," Polton added.

Uri Halperin, chief executive officer at ISTEC, an Israeli cybersecurity firm, and former head of national security in the Israeli Prime Minister's Office, echoed these sentiments. Iran, he said, is one of the chief sources of state-sponsored attacks on Israel.

“Most of this is coming probably from Iran, although the Iranians have managed to camouflage some attacks as if they come from other countries,” Halperin said. “We know for sure that it’s Iranian retaliation to what they consider Israeli attacks against them.” The Technion—Israel Institute of Technology fell victim to one such attack just four months ago.At first, Gertler said, the attack appeared motivated by a desire for financial gain. Further investigation, however, suggested it was a politically motivated Iranian attack.

“The first letter imitated a ransomware attack, asking for money. But when we investigated, we quickly realized that there was a state behind the attack,” and that state was Iran. Gertler believes the Technion attack aimed “to embarrass, obtain information, and harm the other party.” But in this instance, the target was “not the Technion, but rather the state of Israel.”

Gertler noted that Iranian-backed cyberattacks do not only target Israel. In July 2022, for example, a group attacked Albanian government websites. A later US investigation said the attackers were probably Iranian-backed, and that they targeted Albania because of its ties to Mujahideen E-Khalq, an Iranian opposition group.

Artificial intelligence (AI) is rapidly changing the nature of cyberattacks and defense. “Both attackers and defenders enjoy what AI has to offer,” said Gertler.

According to Polton, cyberattackers use AI to identify and exploit new vulnerabilities, making it harder for defenders “to keep up” as quickly as needed.

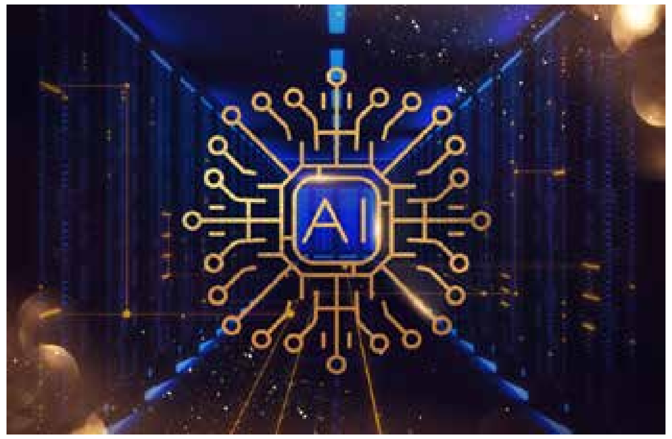
States and private companies must maximize collaboration to face these new challenges, Gertler said. Although balancing the need to share with the need to prevent data breaches can be challenging, “we don’t have a choice,” Gertler argued. “We must be open and collaborate, not just government to government, but within the private sector” as well.

THE JERUSALEM POST

Israel State Comptroller outlines plan to mitigate the huge risk posed by AI

Englman laid out the State Comptroller’s plan to assess the readiness, regulation, and implementation of AI in public-state systems.

By ZACHY HENNESSEY



During his speech at the second day of Cyber Week 2023, Israel State Comptroller and Vice President of EUROSAI Matanyahu Englman warned about the dangerous potential of artificial intelligence, and announced his intention to place the field of cybersecurity at the forefront of the State Comptroller’s audit, noting the grave importance of the government’s preparation for AI-based risks.

“The world is in an arms race towards AI,” he said. “The risks of AI can destabilize our world and affect humanity as a whole – AI tools could be used by hostile elements, such as terrorists and criminals, and cause tremendous damage.”

“The race for AI has led various countries around the world to making huge investments in the field. To emphasize the risks involved, it is enough to mention estimates that two of the four leading countries in the field are China and Russia,” he continued, noting that the leaders of these countries have made public statements regarding the power of being an AI leader. “Alongside the countries, the world’s leading technology companies as well invest billions of dollars to enable a free environment for the development of AI tools.”

Englman went on to note that, since its release to the public on November 30, 2022, Chat-GPT has become the figurehead of the AI movement, having accumulated over 100 million users in just 60 days. By comparison, he pointed out, leading social media platform Facebook took four and a half years to hit the same user milestone.

He highlighted three major risks presented by AI developments: “One is our inability to know whether the information we receive is true or false, as we already live in a world rampant with fake news. Another main risk

is autonomous weapons in the wrong hands – terrorist organizations, organized crime etc. Other major risks involve the labor market in which many jobs will disappear while a demand will be created for others," he said.

"In order to deal with the multitude of risks, regulation is required, which many countries have only just begun to establish. It appears that the European Parliament is the most advanced, having just recently passed legislation. The Israeli government must get involved in this matter," he said.

Englman laid out the State Comptroller's plan to assess the readiness, regulation, and implementation of AI in public-state systems. The plan focuses on three crucial aspects that warrant attention:

The first aspect pertains to technology. The audit office aims to determine whether the government is adequately prepared for the advancements and challenges presented by AI. This includes evaluating the government's governance structures, computing capabilities, and human capital to ensure they align with the demands of AI integration. Additionally, the plan emphasizes the need to examine the information and data upon which AI systems base their decisions, aiming to shed light on the often-opaque nature of AI algorithms.

The second aspect of the audit plan revolves around regulation and legislation. Recognizing the potential adverse effects and dangers associated with AI, the government seeks to safeguard its citizens and itself by implementing appropriate restrictions on AI technology. This proactive approach aims to strike a balance between leveraging AI's benefits and mitigating any potential harm or misuse.

The third and final aspect focuses on the implementation of AI within the public-state systems. The audit office intends to assess how AI has been assimilated across various national sectors, such as health, law, defense, and education. By evaluating the extent and efficacy of AI integration, the government aims to identify areas of improvement, address potential challenges, and optimize the benefits of AI adoption in these critical domains.

"The auditing world views AI as involving major risks. The challenges involved in coping with the issue are complex and require, among other things, continuous cooperation between states," Englman concluded. "We in the State Comptroller's Office are committed to continue addressing this significant topic even more vigorously, for the benefit of the citizens of Israel and the entire world."

Cyber Week 2023 is the latest iteration of the annual conference which convenes cybersecurity experts and executives from around the world in order to discuss the state of the cybersecurity industry and look toward its future.

THE JERUSALEM POST

IDF will run entirely on generative AI within a few years - Israeli cyber chief

"I estimate that within a few years, every area of warfare will be based on generative AI information," Maj.-Gen. Eran Niv said.

By YONAH JEREMY BOB

IDF Information Technology and Cyber Commander Maj.-Gen. Eran Niv on Wednesday said that he expects that the entire military will run on generative artificial intelligence (AI) within a few years.

Speaking at the Tel Aviv University Cyber Week Conference, Niv said, "Artificial intelligence is a phenomenon which is trending and expanding, with a focus on generative AI. This is a revolution which is increasing our capabilities, but in parallel increasing our reliance on digital infrastructure in every area."

"I estimate that within a few years, every area of warfare will be based on generative AI information. Without a strong and effective digital basis, no one will be able to prosecute a war in any area," said the IDF cyber chief.

Niv stated, "Without a strong digital basis, we will not be able to manage large operations."

Next, he said, "In the modern battlefield, all of the tools, from drones to tanks to sea vessels, and others, can transfer information to all of the other platforms and all of them will be interconnected. This is the vision of establishing a digital front for the battlefield."

Continuing, he stated, "The digital arena will transform all of the other areas of war into being stronger – in the air, in the sea, and on the land."

BLEEPINGCOMPUTER

New Mockingjay process injection technique evades EDR detection

By Bill Toulas

A new process injection technique named 'Mockingjay' could allow threat actors to bypass EDR (Endpoint Detection and Response) and other security products to stealthily execute malicious code on compromised systems.

Researchers at cybersecurity firm Security Joes discovered the method, which utilizes legitimate DLLs with RWX (read, write, execute) sections for evading EDR hooks and injecting code into remote processes.

Process injection is a method of executing arbitrary code in the address space of another running process that is trusted by the operating system, hence giving threat actors the ability to run malicious code without being detected.

Examples of process injection techniques include DLL injection, PE (portable executable) injection, reflective DLL injection, thread execution hijacking, process hollowing, mapping injection, APC (asynchronous procedure call) injection, and others.

In all these techniques, the attackers must use Windows APIs and various system calls, create processes/threads, write process memory, etc. Hence, security tools monitoring for specific actions relating to the above can detect suspicious incidents and intervene as required.

Security Joes says that Mockingjay stands out from other approaches because it does not use commonly abused Windows API calls, set special permissions, perform memory allocation, or even start a thread, hence eliminating many possible detection opportunities.

Devising Mockingjay

The researchers' first goal was to find a vulnerable DLL with a default RWX section, so they could modify its contents to load malicious code without performing extra steps like gaining additional permissions, which could raise red flags on security software.

In their quest for a suitable DLL, the Security Joes analysts discovered the DLL msys-2.0.dll inside Visual Studio 2022 Community, which had a default RWX section of 16 KB in size.

"By leveraging this pre-existing RWX section, we can take advantage of the inherent memory protections it offers, effectively bypassing any functions that may have already been hooked by EDRs," reads the report

"This approach not only circumvents the limitations imposed by userland hooks but also establishes a robust and reliable environment for our injection technique."

Next, the team developed two injection methods, one for self-injection and one for remote process injection.

In the first case, a custom application ("nightmare.exe") loads the vulnerable DLL directly into its memory space using two Windows API calls, granting it direct access to the RWX section without performing memory allocation or setting the permissions.

Next, a clean system module, NTDLL.DLL, is abused for extracting syscall numbers which are then used to bypass EDR hooks using the "Hell's Gate EDR unhooking" technique, letting the injected shellcode run without getting detected.

The second method involves exploiting the TWX section of msys-2.0.dll to inject a payload into a remote process, specifically the "ssh.exe" process.

The custom application launches ssh.exe as a child process, opens a handle to the target process, and injects the malicious code onto the RWX memory space of the vulnerable DLL.

Finally, the injected shellcode loads the "MyLibrary.dll" DLL file, establishing a reverse shell with the attacker's machine as an attack example.

Tests showed that this remote injection attack, which doesn't require creating a new thread within the target process, allocating memory, or setting permissions, successfully evades EDR solutions.

Both methods proposed in Mockingjay use Windows APIs such as 'LoadLibraryW,' 'CreateProcessW,' and 'GetModuleInformation' to load a misconfigured DLL and find the address of the DLL's RWX section.

However, EDRs commonly monitor APIs such as 'WriteProcessMemory,' 'NtWriteVirtualMemory,' 'CreateRemoteThread,' or 'NtCreateThreadEx,' which are more commonly invoked in traditional process injection attacks. Hence, Mockingjay is less likely to raise alarms.

The development of 'Mockingjay' by Joes Security is another indication of why organizations must adopt a holistic security approach instead of solely relying on current EDR solutions.

i24 NEWS

Israel's Shin Bet chief: 'We identified significant number of threats using AI'

Traditional security organizations are required to adapt to the new situation, where any angry person with access to the Internet may become a threat, Bar says

Head of Israel's Shin Bet domestic security agency Ronen Bar said on Tuesday, at the annual International Cyber Week conference hosted by Tel Aviv University, that the agency is effectively using AI technology to prevent terror threats.

"The AI technology was assimilated into the Shin Bet's countermeasures machine naturally. We identified a significant number of threats using AI," Bar said, adding that "in order to make sure that AI will lead to evolution and not revolution, we will need cooperation and openness between the technology giants and the security agencies."

"Traditional security organizations are required to adapt to the new situation, where any angry person with access to the Internet may become a threat," he said.

Bar noted that they realized that it was impossible to "win this war with sticks and stones." He gave an example of the Lion's Den terrorist recently killed by Israeli forces, noting that "he was born from the smartphone camera, not inside a mosque."

"We are in the depths of the network and see very well what is happening in it: espionage, terrorism, incitement, and foreign influence. The network, like the terrorists' nests in Jenin and the terror tunnels in Gaza, is not a safe space for our enemies," Bar said.

"The Iron Dome that the Shin Bet is developing in cyberspace is already taking its first steps, the array of alliances is emerging and it has already come into action. We are already cooperating with a number of significant countries in the field and we see the global cyber iron dome beginning to take shape," he stressed.

i24 NEWS

Emirati official reveals Israel helped repel a cyber attack on the Gulf state

UAE cyber security head, Mohamed Al-Kuwaiti, says the Israelis and 'its many companies have helped us and are still helping us to build a cyber iron dome'

The United Arab Emirates (UAE) cyber security head, Mohamed Al-Kuwaiti, said Israel and "its national cyber system" helped repel a cyber attack against the Gulf state, Kan reported on Thursday.

During a speech at the Cyber Week conference this week in Tel Aviv, Al-Kuwaiti said "Israel and its national cyber system helped us repel a DDo denial-of-service cyber attack." He went on to thank the Jewish state for setting up the "cyber Iron Dome."

"The great start-up nation (Israel) and its many companies have helped us and are still helping us to build a cyber iron dome or improve the existing one," he said.

The national cyber systems of Israel and the UAE, along with dozens of cyber systems in other countries, have launched a global information-sharing platform to combat hacking and ransomware. "We face common challenges in the cyber field," said Israel's head of the national cyber system, Gabi Portnoy.

"The attack surface is expanding with new technologies and the growing motivation of cyber attackers. We must meet the challenges with our partners, using the knowledge we have acquired and new technologies for better and faster protection," Portnoy added.

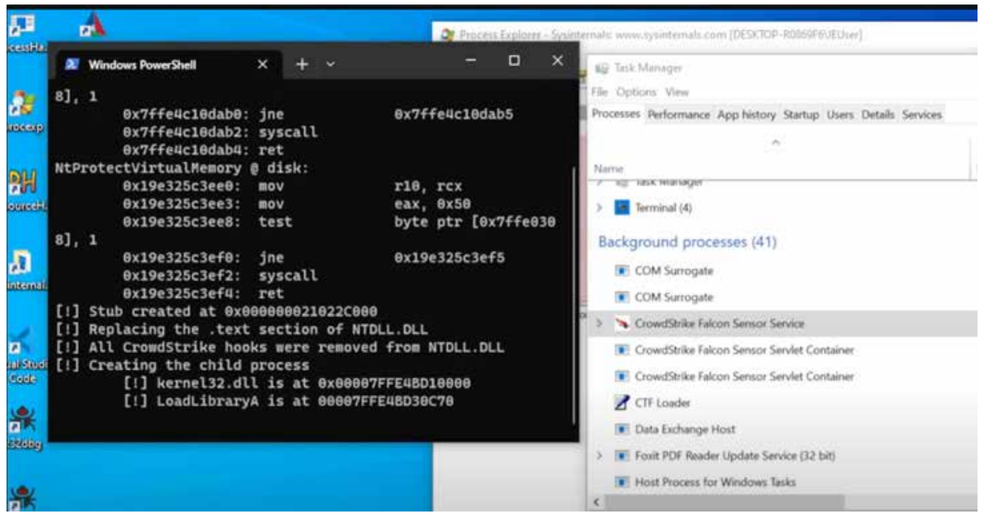
Following a 2020 normalization agreement between Israel and the UAE, as part of the Abraham Accords, the nations also embarked on a series of cooperative ventures. In addition, tourism has also boomed, with an estimated 150,000 Israelis visiting the Gulf state in 2022.

"The historic peace accord we signed with the UAE continues to bear fruit for the benefit of the citizens of both countries," Israeli Prime Minister Benjamin Netanyahu commented on the budding relationship, during a signing of an economic agreement in March.

The Hacker News™

New Mockingjay Process Injection Technique Could Let Malware Evade Detection

Ravie Lakshmanan



A new process injection technique dubbed Mockingjay could be exploited by threat actors to bypass security solutions to execute malicious code on compromised systems.

"The injection is executed without space allocation, setting permissions or even starting a thread," Security Joes researchers Thiago Peixoto, Felipe Duarte, and Ido Naor said in a report shared with The Hacker News. "The uniqueness of this technique is that it requires a vulnerable DLL and copying code to the right section."

Process injection is an attack method that allows adversaries to inject code into processes in order to evade process-based defenses and elevate privileges. In doing so, it could allow for the execution of arbitrary code in the memory space of a separate live process.

Some of the well-known process injection techniques include dynamic link library (DLL) injection, portable executable injection, thread execution hijacking, process hollowing, and process doppelgänging, among others.

It's worth pointing out that each of these methods requires a combination of specific system calls and Windows APIs to carry out the injection, thereby allowing defenders to craft appropriate detection and mitigation procedures.

What sets Mockingjay stands apart is that it subverts these security layers by eliminating the need to execute Windows APIs usually monitored by security solutions by leveraging pre-existing Windows portable executable files that contain a default memory block protected with Read-Write-Execute (RWX) permissions.

This, in turn, is accomplished using msys-2.0.dll, which comes with a "generous 16 KB of available RWX space," making it an ideal candidate to load malicious code and fly under the radar. However, it's worth noting that there could be other such susceptible DLLs with similar characteristics.

The Israeli company said it explored two different methods -- self injection and remote process injection -- to achieve code injection in a manner that not only improves the attack efficiency, but also circumvents detection.

In the first approach, a custom application is utilized to directly load the vulnerable DLL into its address space and ultimately execute the desired code using the RWX section. Remote process injection, on the other hand, entails using the RWX section in the vulnerable DLL to perform process injection in a remote process such as ssh.exe.

"The uniqueness of this technique lies in the fact that there is no need to allocate memory, set permissions or create a new thread within the target process to initiate the execution of our injected code," the researchers said.

"This differentiation sets this strategy apart from other existing techniques and makes it challenging for Endpoint Detection and Response (EDR) systems to detect this method."

The findings come weeks after cybersecurity firm SpecterOps detailed a new method that exploits a legitimate Visual Studio deployment technology called ClickOnce to achieve arbitrary code execution and obtain initial access.

Head Of Cyber Security Leads A UAE Delegation To Cyber Week In Tel Aviv

Muhammad Irfan

(UrduPoint / Pakistan Point News / WAM - 29th Jun, 2023) ABU DHABI, 29th June, 2023 (WAM) – Dr. Mohamed Al Kuwaiti, Head of Cyber Security for the Government of the UAE, led a high-level UAE delegation of dozens of participants from leading Emirati entities to Cyber Week 2023 Conference in Tel Aviv.

Dr. Mohamed Al Kuwaiti addressed the Cyber Week Conference as a key-note speaker in the main plenary panel titled "Safeguarding the Nation: Cybersecurity Strategies for a Digital Age", along with Gaby Portnoy, Director General of the Israel National Cyber Directorate, and several top international government officials.

During the visit, the UAE delegation met with the central cyber stakeholders in the Israeli cyber ecosystem including investors, Chief Information Security Officers and top cyber experts, and visited leading cyber labs and R&D centers and startups to explore opportunities to deepen the ongoing partnerships.

The visit provided valuable insights into the latest global trends in cybersecurity and allowed the participants to explore potential collaborations and bilateral investment opportunities.

Al Kuwaiti said: "Cyber security is a shared responsibility that can never be addressed by one person, organization or country alone. Instead, it requires mutual collaboration between the private and public sectors.

Partnership with the industry and academia is critical as it brings all the stakeholders of the digital ecosystem together with a common vision. Our goal is to spread the cyber security culture.

The end result will be a more secure, more resilient digital future, not only for the UAE but for our partners and friends."

Mohamed Al Kuwaiti, represents the ongoing collaboration between Israel and the UAE in the cybersecurity domain, as both nations recognize the critical importance of a secure and resilient digital infrastructure.

Israel remains committed to nurturing these relationships and promoting cross-border partnerships in cybersecurity and beyond."

On the sidelines of the Cyber Week conference, the UAE-based EliteCISOs, a global cyber security community, signed a Memorandum of Understanding (MoU) with the Israel-based Cyber Together, an Israeli NGO, to expand this global community to Israel.

This MoU marks the beginning of a strategic partnership aimed at fostering cooperation in the field of cybersecurity between key professionals in both countries.

The signing event was held in the presence of Dr.

Mohamed Al Kuwaiti, Head of Cybersecurity of the UAE Government and Oded Joseph, Deputy Director General, Head of middle East Division in the Ministry of Foreign Affairs, Israel.

Oded Joseph: "Israel is fully committed to fostering collaborations and partnerships with the United Arab Emirates between the various ecosystems of innovation of our nations.

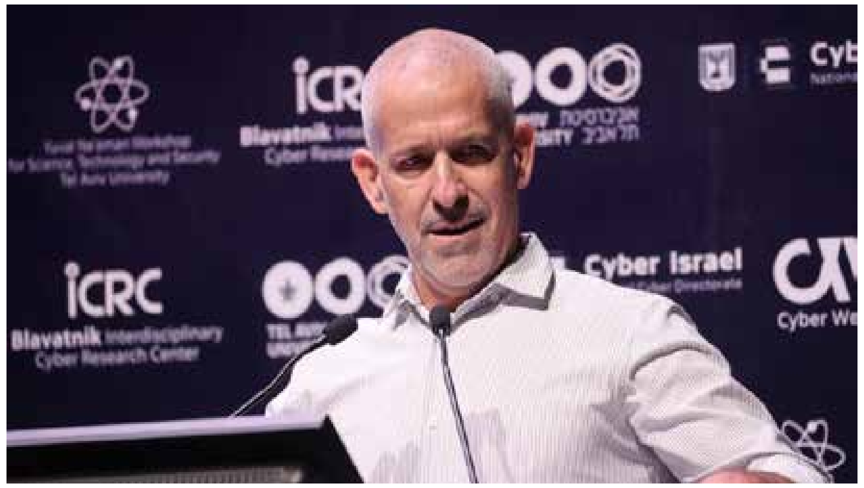
This MoU, a strategic partnership between two leading cyber security stakeholders, further strengthens our relations and represents the shared benefits of the Abraham Accords beyond the relationship between governments to partnerships between organizations and people."

Under the terms of the MoU, EliteCISOs and Cyber Together will collaborate on various initiatives including knowledge-sharing, joint training and workshops to enhance cybersecurity capabilities, promote the development of a highly skilled cybersecurity workforce and address emerging threats in both the UAE and Israel.

The relationship between EliteCISOs and Cyber Together was initiated and fostered by the Consulate-General of Israel in Dubai as part of its wider effort to establish new cyber-based partnerships between entities in the two countries.

Shin Bet develops ChatGPT-like tool for detecting threats, chief Ronen Bar says

Shin Bet head says AI enables his agency to create an effective defense barrier against Israel's enemies, as well as assisting the organization in streamlining operations, prioritizing tasks, intelligence gathering, decision-making, and prediction



Shin Bet Director Ronen Bar revealed Tuesday that the agency developed an AI-based chatbot resembling ChatGPT for internal purposes.

Speaking at the Cyber Week event at Tel Aviv University, Bar said: "AI technology was naturally embedded in Shin Bet's counterterrorism mechanism. Using AI, we have identified a significant number of threats, and the device's ability to detect anomalies creates an effective defense barrier against our enemies, alongside the traditional capabilities of the Shin Bet, including human intelligence, signals intelligence, cyber, intelligence analysis and operations."

According to Bar, the Shin Bet also identifies threats posed by artificial intelligence, and also recognizes the opportunities it presents. "As part of implementing the technology in the organization, we have established the Gen AI On-Prem capability (generative artificial intelligence located on the organization's servers)," he revealed. "The capability is accessible to employees in an intuitive manner, and it can be interacted with similarly using familiar tools on the web, such as Gboard (Google's chatbot) and ChatGPT."

Bar also says that artificial intelligence assists the organization in streamlining operations, prioritizing tasks, intelligence gathering, decision-making and prediction.

Bar also addressed the challenges posed by artificial intelligence to the agency. The first challenge is the availability of technology, which, according to Bar, "is everywhere, in the hands of every person, country and organization, whether they are good or bad. Developing nuclear capabilities once required significant resources, but AI, with its enormous potential for harm, requires nothing more than a mobile device and an internet connection."

The second challenge, as Bar defines it, is the "temptation." This, according to Bar, means

that it "can be assumed that generative artificial intelligence will be able to tempt the user, most likely by delivering information quickly, extensively and without moral restraints, at the expense of accuracy and depth. As the user consumes content, the AI will provide them with the answers they want to hear. Since artificial intelligence will cater to the user's desires, it can be assumed that it will provide dangerous knowledge that, in one way or another, could fall into the wrong hands."

The third challenge that Bar discussed is the "lack of accountability."

"On the web, and also in AI, the basic normative requirement in every relationship system and in every society, which is accountability, does not apply. In the absence of accountability, only the 'law of the jungle' applies. Therefore, we will need to adapt Israeli regulation, redefine what constitutes secrecy, update the Shin Bet Law that was written in the SIGINT era to the cyber and AI era, and continue to be agile in the field of technology," Bar said.

"In order to ensure that AI leads to evolution and not revolution, we will need cooperation and openness between technology giants and security bodies," Bar said. He added that Shin Bet intends to establish a hub that will focus on generative artificial intelligence and assist startups and entrepreneurs in developing products that can meet security needs.

ynet ידיעות אחרונות

No paruski: Israeli cyber chief vows vengeance against Iranian hackers, skirts around Russia threat

Gabi Portnoy zeroes in on Tehran as primary threat to Israel's digital infrastructure but forgoes any mention of Russian-linked offensive cyber activities in recent months
Raphael Kahan

Brigadier Gen. Gabi Portnoy, head of the National Cyber Directorate (NCD), delivered on Tuesday a speech highlighting the threats to the country's digital infrastructure and issued a strong warning directed at Iran, but notably omitted any mention of similar threats originating from Russia.

Speaking at Tel Aviv University, Portnoy said that those launching cyber attacks on Israeli civilians, namely Iran and Hezbollah, should anticipate consequences. However, he conspicuously dodged any mention of Russia, which has targeted Israeli networks via Kremlin-linked hacker groups and intelligence services multiple times over the past year.

In response to a Ynet request for comment about Portnoy's omission of Russia, the NCD said they are vigilant and ready to counter all attacks and attackers without explicitly attributing them to specific entities, including private companies.

This approach of eluding any mention of Russia mirrors the government's policy of maintaining strategic ambiguity and maintaining full diplomatic relations and cooperation with Moscow for various political considerations.

Conversely, in a subsequent speech by Kemba Eneas Walden, the White House's cyber director and advisor to President Joe Biden, both Russia and China were acknowledged as major cyber threats to the Western world.

Portnoy addressed the MuddyWater hacker group, linked to Iran's Ministry of Intelligence and Security, highlighting their extensive activities beyond Israel. He emphasized their attacks on civilian targets in numerous countries, including Turkey, Saudi Arabia, Egypt, Morocco, India, Bahrain, Oman, Kuwait and more.

Portnoy noted that Israel's cyber community is well-acquainted with Iran's cyber operations and actively works to disrupt them, naming specific individuals from the Iranian Intelligence Ministry, the Islamic Revolutionary Guard Corps and Hezbollah involved in cyber operations against Israel.

During his speech, Portnoy outlined the recent efforts in enhancing resilience and safeguarding the economy. He highlighted several initiatives, including the Cyber-Dome project — a new big data, AI, overall approach to proactive cyberdefense.

Portnoy also mentioned a collaborative endeavor with Microsoft and the United Arab Emirates to establish a platform for cyber investigations and knowledge-sharing involving some 40 countries. The initiative align

with the White House's forum to combat ransomware attacks.

THE WEEK

How India, UAE, Israel are trying to build secure cyberspace

UAE cyber security head had recently visited India and Israel
By Namrata Biji Ahuja

DR MOHAMED AL KUWAITI has been a busy man, of late. Kuwaiti, head of cyber security for the government of the United Arab Emirates, has been on his toes, what with the UAE being hard at work at cementing the India-UAE-Israel partnership for shaping a new Middle East. The partnership is based on regional security integration to beat common threats. The three countries are also building alliances to strengthen economies by creating food corridors and inking agreements on energy, transportation, trade and health care.

For all future projects and partnerships, securing the digital space is key, and the cyber security heads of the three countries are joining forces. Take, for instance, Israel, which has cutting-edge technologies at its disposal. "Artificial intelligence is helping us create an Iron Dome in the Israeli cyber security space," said Ronen Bar, director of Israel Security Agency, which is also known as the Shin Bet. Creating a cyber dome that goes beyond Israel's cyberspace to help its partners is not a distant thought. And, it is wooing the UAE big time.

In the last fortnight, Kuwaiti travelled to two ends of a geostrategically significant arcIndia and Israel. He carried a basketful of innovative ideas and technology for cooperation in cyber security to the two countries. His visit is symbolic in light of the I2U2 (India, Israel, the UAE and the US) grouping, reaffirming support to the Abraham Accords for Israeli-Emirati normalisation that transcends political or regional challenges.

New Delhi is an active partner in this strategic convergence. Predictably so, Kuwaiti's first stop was India. He held hectic closed-door meetings with top cyber security officials of India's National Security Council Secretariat with the aim to maximise innovation, entrepreneurial dynamism and technology in all four countries.

Top government sources said an India-UAE cyber partnership is in the works to create opportunities for both public and private sectors in the digital arena. This is besides offering innovative solutions for growing threats to the cyber security ecosystem that go beyond geographical boundaries and even human imagination. Israel is using its research and development labs in the Ben-Gurion University of the Negev in Be'er Sheva, its cyber capital, to create solutions for imminent threats from the misuse of AI, ChatGPT and the Internet of Things. With AI already being used for running trains and driverless buses, building smart homes and regulating water, power and all essential supplies and critical infrastructures, governments around the world can ill afford to be manipulated, said Dr Isaac Ben, director of Interdisciplinary Cyber Research Center at Tel Aviv, who is considered the father of cyber security in Israel.Moreover, radical terror groups like the Islamic State the first terrorist organisation that recruited, trained and organised real-time terror attacks using online platforms and its affiliates are a threat to the entire region. Besides this, the growing military and cyber heft of China has

given enough reason to New Delhi to review its cyber preparedness in an entirely new way. And, it is looking at the UAE and Israel to play a huge role in securing its digital space and strengthening national security. It is the UAE's moment under the sun, with Kuwaiti pitching Emirates as a hub for Israel to share its cutting-edge technological advancements and cyber security prowess, opening a floodgate of tie-ups between the two. "Cyber security is a shared responsibility that can never be addressed by one person, organisation or country alone," said Kuwaiti, who attended the annual Cyber Week Conference at Tel Aviv. "Instead, it requires mutual collaboration between the private and public sectors. Partnership with the industry and academia is critical as it brings all stakeholders of the digital ecosystem together with a common vision." The end result, he said, will be a more secure, resilient digital future, not only for the UAE but also for its partners and friends.The US cannot agree more. Whether it is Russia's assault on Ukraine or Iran's recent cyber attack on Albania's critical digital infrastructure, the US is well aware of the fast-evolving dangers in cyberspace. Nathaniel C. Fick, US ambassador-at-large for cyberspace and digital policy, said joint efforts with Israel to build a defensible, resilient and rights-respecting digital ecosystem is the way forward. For all countries, trust is important, which is why Kuwaiti has been on a mission to give a personal touch to the bonding in cyberspace. The outcome has been promising. The UAE and Israel have decided to create a skilled workforce in cyberspace that understands the common threats and jointly blocks them. The UAE-based EliteCISOs, a global cyber security community, signed a memorandum of understanding with Cyber Together, an Israeli NGO. "This MoU, a strategic partnership between two leading cyber security stakeholders, further strengthens our relations and represents the shared benefits of the Abraham Accords beyond the relationship between governments to partnerships between organisations and people," said Oded Joseph, deputy director general, head of Middle East Division in the ministry of foreign affairs of Israel.

India is not far behind and the next big partnership for New Delhi is being readied during GITEX Global, the world's largest tech showcase in Dubai in October. The event will bring Israel, India and the rest of the world to the UAE and create new opportunities for technical collaboration in the region.

THE WEEK

Iran faces heat as world looks at naming and shaming threat actors at Israel's global cyber meet

The era of nameless, faceless cyber attacks is over

By Namrata Biji Ahuja

The global cyber defence strategy took shape in this part of the world when Israel became the first country "to come out of the closet" making cyber technology a legitimate civilian way of life. Once again, it is the Israelis leading the way into a robust space of cyber defence and offence, naming and shaming threat actors and putting together the best brains to beat new-age threats from targeted misuse of Artificial Intelligence.

The era of nameless, faceless cyber attacks is over. The Israel National Cyber Directorate announced before a packed audience of representatives from across continents attending the Cyber Week in Tel Aviv on June 27, "Anyone who carries out cyberattacks against Israeli citizens must take into account the price he will pay.''

For more than a decade, countries have been debating the so-called 'name and shame' tactic or 'attributing' cyber attacks as a deterrent to unwanted cyber behaviour but none have come out as strongly in their fight back as Israel.

Gaby Portnoy, Director General of Israel National Cyber Directorate, said, "In the past year, we have been working hard to develop our resilience and expand our capabilities to detect cyberattacks, raising our shields and expose malicious activities, specifically Iranian."

According to Portnoy, the vast majority of attacks are thwarted. He mentioned the attack in February that forced the Israel Institute of Technology, also known as Technion, to postpone exams and temporarily shut down its IT systems and attributed it to MuddyWater in collaboration with Darkbit-- two attack groups associated with the Iranian Ministry of Intelligence. He said, "They are also attacking civilian targets in countries like Turkey, Saudi Arabia, Egypt, Morocco, India, Oman, Bahrain, Kuwait and more."

Portnoy said the Israeli defence community knows the Iranian cyber activities inside out and is working to disrupt them in different ways. From naming the Iranian intelligence and Hezbollah, to commending the United States for imposing sanctions on Iranian officials, the message was clear. Israel was preparing its 'cyber dome' project by inviting friendly nations to participate.

"I would like to commend the US activities against Iran's violent agenda and for imposing sanctions against two active cyber players in the Ministry of Intelligence and Security: Mojtaba Mostafavi and Farzin Karimi, who co-founded the Ravin Academy that trains hackers for malicious activities of the ministry." The threats from elements in Beirut linked to Hezbollah, according to Portnoy, were damaging civilian lives across the world and to stop it, the international community needed to work together. "This is our joint responsibility."

It is indeed a shift in global cyber strategy for many countries, including India, where cyber attacks are reluctantly

spoken of publicly and governments are shy to admit offensive capabilities.

Portnoy is helming efforts in his country helping high school kids, small and medium enterprises and critical infrastructures like transport, hospitals, and banks to not just learn how to defend, but also assist the half a dozen security and intelligence agencies in effectively battling and exposing malicious activities and threat actors.

The United States, among others, clearly understands the fast-evolving dangers in cyberspace. Nathaniel C Fick, the ambassador at large for cyberspace and digital policy in the US Department of State spoke of joint efforts with Israel to implement an affirmative vision for a secure cyberspace and building a defensible, resilient and rights-respecting digital ecosystem.

The former combat marine said “With power comes responsibility” especially for countries with advanced capabilities .“We must award responsible behaviour and impose costs on irresponsible behaviour.” Fick stressed on a shared technology ecosystem where trust is paramount and reminded all United Nations members of their commitment to building a framework for responsible state behaviour.

“It’s universal. Technology innovation benefits with greater participation,” he said. Israel has endorsed the Declaration for the Future of the Internet with the US and sixty-five partners around the globe, launched last year to reaffirm and recommit to a single global Internet that is truly open and fosters competition, privacy and respect for human rights. Fick said it also articulates what a shared tech policy can and should be. He said border coalitions of countries have condemned Iran for its cyber attack on Albania’s critical digital infrastructure and Russia’s assault on Ukraine and provide assistance to mitigate future attacks. The thorny aspect of commercial spyware was also touched upon by Fick, who said the growing private market in these technologies, where it can be used as a tool of repression and human rights abuse needs to be countered by deeper international cooperation. He said a recent executive order in the US prohibits the operational use of commercial spyware that poses a risk to national security or has been used by foreign actors and urged countries to adopt similar measures.

Lastly, he said public attribution of malicious cyber activity, which is empirical and factual, is the key to building a rules-based order. From being technical to a rather political challenge, he said there is a need for more countries to join the US in lending voices to public attribution on a case-to-case basis.

DARKReading

Mockingjay Slips By EDR Tools With Process Injection Technique

By leveraging misconfigured DLLs instead of EDR-monitored APIs, this new technique injects malicious code into running processes, completely evading endpoint security.
Jai Vijayan

Endpoint detection and response (EDR) systems have become increasingly efficient at detecting typical process injection attempts that invoke a combination of application programming interfaces to insert code into the memory space of a running process.

So researchers at Israeli-based Security Joes set out to find another way to due process injection without relying on EDR-monitored APIs. The result is Mockingjay, a novel method for process injection that leverages dynamic link libraries (DLLs) with default read, write, and execute (RWX) permissions to push code into the address space of a running process.

The Mockingjay Approach

The approach reduces the likelihood of an endpoint security mechanism detecting a malicious process injection effort and requires a smaller number of steps to achieve, Security Joes said in a report this week. “Our research aimed to discover alternative methods to dynamically execute code within the memory space of Windows processes, without relying on the monitored Windows APIs,” the security firm said.

“Our unique approach, which involves leveraging a vulnerable DLL and copying code to the appropriate section, allowed us to inject code without memory allocation, permission setting, or even starting a thread in the targeted process.”

Process injection is a technique for manipulating the memory of a process to either add new functionality or modify its behavior. Attackers commonly use the method to hide malicious code and evade detection on compromised systems. Common process injection methods include self-injection where a process that receives the injected payload also executes it; DLL injection where a malicious DLL is loaded into the memory space of a process; and PE injection where a portable executable file is mapped into the memory of a running process.

“Each of these injection techniques requires a set of specific Windows APIs, which generate characteristic patterns that can be leveraged by defenders and security software for detection and mitigation purposes,” Security Joes said in its report. For instance, the APIs required for self-injection are VirtualAlloc, LocalAlloc, GlobalAlloc, and Virtual Protect, the company said. Similarly, the APIs used in PE injection are VirtualAllocEx, WriteProcessMemory, and CreateRemoteThread. Most EDR systems are tuned to monitor commonly used APIs in process injection attacks and can effectively identify malicious activity associated with their use.Abusing Vulnerable DLLs

DARKReading

The strategy Security Joes used in developing Mockingjay was to systematically search for DLLs within the Windows OS that contained a default RWX section. Researchers at the company developed a tool that explored the entire Windows file system to identify DLLs that could serve as potential vehicles for code injection without triggering an EDR alert. The exploration resulted in Security Joes finding a DLL (msys-2.0.dll) with 16KB of RWX space in Visual Studio 2022 Community that they could use for injecting and executing their own code.

"After identifying the vulnerable DLL that contains a default Read-Write-Execute (RWX) section on disk, we conducted several tests to explore two different methods that could leverage this misconfiguration to execute code in memory," Security Joes said.

One method was to directly load the vulnerable DLL into the memory space of a custom application called nightmare.exe that Security Joes developed. Doing that allowed researchers to inject and execute their own shellcode into the memory space of the application without leveraging any Windows APIs. Among other things, the shellcode also removed all EDR hooks without triggering any alerts. "This complete removal of dependency on Windows APIs not only reduces the likelihood of detection but also enhances the effectiveness of the technique," the company said.

Security Joes' second tactic for abusing the RWX section in the DLL was to do process injection in a remote process. To achieve this, they first identified binaries that used mysys-2.0.dll for their operations. Many of these were associated with GNU utilities and other applications that require POSIX emulation. For the proof-of-concept, researchers chose the ssh.exe process in Visual Studio 2022 Community as the target for injecting their code. "It is important to note that in this injection method, there is no need to explicitly create a thread within the target process, as the process automatically executes the injected code," the company explained.

According to Security Joes, the DLL that its researchers used to developed Mockingjay is just one of potentially many others that can similarly be abused for code injection purposes. Addressing the threat requires endpoint security tools that don't just monitor specific APIs and DLLs but also use behavioral analysis and machine learning techniques to identify process injection.

UAE, Israel Ink Pivotal Joint Cyber-Threat Intelligence Agreement

Two Mideast nations that were at odds until recently have announced the "Crystal Ball" project, aimed at better protecting against cyberattacks via collaboration and knowledge sharing.

Dan Raywood

In a watershed moment for two once-fractious regional neighbors, the United Arab Emirates (UAE) and Israel are to work together on a threat intelligence-sharing platform to battle cybersecurity threats.

Announced this week, the "Crystal Ball" project is a digital platform for detecting and repelling hackers via collaboration and knowledge sharing around national-level cyberthreats. It was described as being enabled to "design, deploy and enable regional intelligence enhancement," according to a presentation slide seen during this week's Tel Aviv Cyber Week.

The project will be backed by Microsoft, Israel's Rafael Advanced Defense Systems, and Abu Dhabi's CPX, and an unspecified number of countries will also participate, according to The Circuit.

The Need for a Joined-up Response

Emirati cybersecurity chief Mohamed Al Kuwaiti said the platform will enable partner countries to "easily and seamlessly share information," and will be strengthened by the combination of the countries' joint abilities, processing power, and a high volume of data.

In an address to the Cyber Week conference, Al Kuwaiti said, "Cyber threats do not distinguish between nations, do not distinguish between entities or people, and that is why we need to unite against those threats. The Crystal Ball that we are aiming for the whole community will be the first step toward that."

Nadir Izrael, co-founder and CTO of Armis, says he welcomes the joint effort in the Middle East because he is "a strong believer that nations need to work together to develop a comprehensive and effective response to cyber warfare, in order to build a more secure and resilient world."

He adds: "As we saw with the cyberattacks on Israel this late April, coordinated efforts from groups associated with Iran and Russia are looking to increase geopolitical tensions and create instability amongst citizens. In a world that has become polarized, it is a must to invest in cybersecurity measures to protect whole nations from these kinds of attacks."

Izrael also noted that the Crystal Ball project should be a model for others. "Governments and organizations need to take threats seriously, and allocate resources to build robust and resilient cybersecurity systems," he says. "Those advanced systems will allow for threat intelligence, which can help detect malicious behavior and stop an attack even before it happens."

Improved Diplomatic Relations

Al Kuwaiti said the UAE's connection with Israeli tech companies has been especially helpful in his country's transition to a digital economy, after the UAE and Israel normalized diplomatic relations as part of the September 2020 Abraham Accords, leading to the bolstering of both commercial and strategic ties between the countries.

Ryan Westman, senior manager of threat intelligence at eSentire, says the collaboration of threat intelligence sharing between Israel and the UAE will be key to better securing the region. "In general, any information-sharing agreement will likely benefit organizations in the countries covered, as the more insights we have on threats and vulnerabilities to organizations, the better the job we can do at responding to those the risk those threats and vulnerabilities present," he says. "By sharing information on those threats and vulnerabilities, the easier it is for security teams to respond to the risks."

He notes that while information sharing and analysis centers (ISACs) have existed for some time now and are not novel, the collaboration between two states that used to be at geopolitical odds is notable.

"Partnerships like this can have a wider impact, improving the security posture for everyone, because it makes it easier to detect potential issues in the wider threat landscape," he says. "Working together in this way benefits everyone, whether they are in the two countries concerned or in others within the region."

CyberSecurity news

Mockingjay – A New Injection Technique to Bypass Endpoint Detection and Response (EDR)

The cybersecurity researchers at Security Joes recently discovered a new injection technique that is dubbed "Mockingjay."

The threat actors could actively exploit this newly discovered injection technique to run and execute malicious code on compromised systems by evading the EDR (Endpoint Detection and Response) and other security solutions.

Utilizing DLLs with RWX sections, this technique easily bypasses the EDR hooks and injects code into remote operations.

By injecting code into trusted running processes, the process injection enables threat actors to execute undetected malicious code.

Attackers employ Windows APIs, system calls, process/thread creation, and process memory writing in these techniques.

Security tools can detect and intervene in suspicious incidents by monitoring specific actions mentioned above.

The following things differentiate the Mockingjay from others that enable it to evade several detection possibilities:-

Commonly abused Windows API calls are not used

Process Injection Methods

Here below, we have mentioned all the process injection methods:-

Self-Injection: This technique is commonly found in malware packers and does not impact any external process; rather, the process executing the injection is the same process that receives the injected payload.

Classic DLL Injection: This technique injects a malicious DLL into the memory space of another process. In this case, the malicious sample must first identify the specific process it intends to target, allocate a portion of memory within it and create a thread to start the execution of the malicious DLL from disk.

PE Injection: This technique maps an entire Portable Executable (PE) file into the memory space of a running process. It allocates a new memory section within the target process, which will serve as the destination for the payload. The contents of the payload are then dynamically mapped onto this memory section using its relocation descriptors and the absolute address of the section, imitating the functionality of the Windows Loader.

Process Hollowing / Run PE: In this technique, the original code and resources of the target process are replaced or removed, leaving behind only the bare process framework. The hollowed process then becomes a host for the injected malicious code, allowing it to execute under the guise of a legitimate process.

Thread Execution Hijacking: This technique is used to gain control of the execution flow within a process by redirecting the execution of a target thread to arbitrary code. It allows an attacker to manipulate the behavior of a running process without creating a new process or modifying the underlying code.

Mapping Injection: By utilizing the NtMapViewOfSection, the malicious code is mapped into the target process from an existing section, controlled by the attacker. This approach eliminates the requirement to explicitly allocate RWX sections and avoids the need for separate payload content copying. The malicious code indirectly becomes part of the target process's memory space, allowing it to execute within the context of a genuine module.

APC Injection and Atombombing: This technique manipulates the Asynchronous Procedure Call (APC) mechanism in the Windows operating system to inject and execute malicious code in a target process.

Process Doppelganging: This technique is used in malware development to disguise malicious processes by creating a process with a legitimate appearance. It involves utilizing transactional NTFS (TxF) and Windows process loading mechanisms to create a new process that looks like an existing, legitimate process but runs malicious code instead.

Mockingjay Bypass EDR

Researchers aimed to locate a vulnerable DLL with a default RWX section, enabling effortless modification of its contents for loading harmful code.

This bypasses the need for extra steps like obtaining more permissions, which may alert security software.

Security Joe's analysts, on their DLL search, stumbled upon Visual Studio 2022 Community's msys-2.0.dll, sporting a 16 KB default RWX section.

Following that, the team devised two injection techniques, and here they are mentioned below:-

Self-injection

Remote process injection

For the initial scenario, "nightmare.exe," a custom application that directly loads the vulnerable DLL using two Windows API calls into its memory.

This bypasses the memory allocation or permission settings and provides direct entry to the RWX section.

While at this point, EDR gets informed about the creation of a new process and promptly adds its own dynamic library to it after the application is launched.

After execution, the EDR alters byte code to modify targeted functions within the in-memory NTDLL.DLL copy. Following that, the "Hell's Gate EDR unhooking" technique exploits NTDLL.DLL, a new system module, to extract syscall numbers.

These numbers bypass EDR hooks, enabling undetected execution of the injected shellcode.

jns Jewish News Syndicate

Four US officials in Tel Aviv for Israel Cyber Week

Nathaniel Fick, ambassador at large for cyberspace and digital policy, is one of three U.S. officials who will speak at the event.

Nathaniel Fick, the inaugural U.S. ambassador at large for cyberspace and digital policy, will deliver remarks at Israel Cyber Week and meet with Israeli counterparts and U.S. and Israeli private sector representatives on a June 26 to 29 trip to Tel Aviv, the U.S. State Department stated.

Per the event's website, Fick's remarks are titled "Capture the Flag: Defending Taiwan's Democracy from Foreign Interference."

Liesyl Franz, U.S. deputy assistant secretary for international cyberspace security, will join Fick at the annual, international event (now in its 13th year), per Foggy Bottom.

"In their bilateral engagements and in Ambassador Fick's formal remarks at the Israel Cyber Week Plenary, they will discuss U.S. efforts to implement an affirmative vision for a secure cyberspace by working with our allies and partners in the region to build a defensible, resilient and rights-respecting digital ecosystem," the department stated.

"Ambassador Fick will also meet with Israeli government officials to discuss our two countries' technology and cybersecurity collaboration as we seek to promote peace and prosperity in the region."

The Israel National Cyber Directorate tweeted that the event, held at Tel Aviv University, drew "10 official delegations, participants from 80 countries, 30 of our representatives among the 400 speakers in about 50 events." Per the event's website, 10,000 attendees are expected.

Yaniv Harel

Ann Dunkin, chief information officer of the U.S. Department of Energy, is scheduled to deliver a keynote, and Cordell Schachter, chief information officer of the U.S. Department of Transportation, is also a scheduled speaker.

jns Jewish News Syndicate

Palestinian terrorists are ’born via smartphones, not mosques’

Groups like Lions’ Den represent "a new type of terrorism," characterized by its use of technology, said Shin Bet chief Ronen Bar.

PESACH BENSON

Today’s Palestinian terrorists are created online, Israel Security Agency (Shin Bet) head Ronen Bar said on Monday.

Speaking at the Tel Aviv Cyber Week Conference, Bar said that terrorists were “born from the smartphone camera, not inside a mosque.”

The annual conference organized by Tel Aviv University brings together leading international cyber figures from the government, tech and academic sectors. Among notable figures addressing the gathering on Monday were Gabi Portnoy, director general of the Israel National Cyber Directorate, Kimba Walden, the U.S. Acting National Cyber Director, and Mohammed al-Kuwaiti, who heads cybersecurity for the United Arab Emirates.

According to al-Kuwaiti, artificial intelligence is being increasingly used by hackers, and states need to match that with AI for protection.

“Many of the attacks are now done automatically, and this is where we need AI to help us detect and deter those attacks,” al-Kuwaiti stressed. Many of his discussions with startups, academics and government officials attending the conference had touched on this, he said.

Bar, addressing the gathering, described the Lions’ Den terror group, based in northern Samaria, as “a new type of terrorism” that bore closer study for its use of technology and social media platforms such as TikTok and Telegram to recruit a new generation of members.

“You can learn about the way countries and terrorist organizations exploit the young generation. The organization recruits online and receives its support from the public in the form of likes,” said Bar.

Explaining the security establishment’s response, Bar said, “The ‘Iron Dome’ that the Shin Bet is developing in cyberspace is already taking its first steps, the array of alliances is emerging and it has already come into action. We are already cooperating with a number of significant countries in the field and we see the global cyber Iron Dome beginning to take shape.”

He also called on lawmakers and social media companies to take stronger measures.

“A democratic, liberal society with a desire for life must produce a binding regulation—a code of ethics, relevant TTM for removing offensive content, refining the algorithm and exposing people to different opinions and lowering the threshold of incitement,” said Bar.

“I am happy to say that recently we are seeing Tiktok’s steps in the right direction, as far as incitement is concerned. Unfortunately, I cannot say similar things about Twitter and Telegram,” he added.

Iranian hackers

Israel National Cyber Directorate head Portnoy pointed a finger at Muddywater, a group of hackers associated with Iran’s Intelligence Ministry, in connection with numerous Middle East cyber attacks.

“The group works not only against Israel, but attacks civilian targets in many countries including Turkey, Saudi Arabia, Egypt, Morocco, India, Bahrain, Oman, Kuwait and more,” though most of the attacks were unsuccessful, he said.

“The people of the Iranian Intelligence Ministry, people from the Islamic Revolutionary Guard Corps and Hezbollah who are involved in cyber operations against Israel know exactly what I’m talking about,” he added.

Portnoy also praised U.S. sanctions against certain Iranian intelligence figures taking a leading role in Tehran’s cyber attacks. Portnoy cited Farzin Karimi and Mojtaba Mostafavi, who founded the Ravin Academy to train hackers. Karimi and Mostafavi were among a number of Iranian leaders sanctioned by the U.S. Treasury in October 2022.

“Also, Ali Khedri, who lives in Beirut and coordinates cooperation between Iran and Hezbollah in order to cause damage to Lebanese citizens in cyberspace. For some people in the Iranian Intelligence Ministry, harming ordinary citizens of the world is part of the routine,” Portnoy added.

He addressed the senior representatives of the international cyber community who were sitting in the hall, saying that “the international community needs to work together to stop people like Karimi, Metzatpoi and Hadari from their malicious activities against the world.”

Portnoy also cited a joint project with the UAE and Microsoft to build a platform for cooperation in cyber investigations and building knowledge between about 40 countries. The initiative is part of a White House forum to combat ransomware attacks.

Israeli State Comptroller Matanyahu Englman, who is also participating in the Cyber Week conference, reported in May that Israeli hospitals were hit with 13 major cyberattacks in 2021, making the health-care sector one of the most targeted by hackers.

To test the preparedness of the hospitals, a team of hackers overseen by the Comptroller's Office staged a controlled penetration of one major hospital, identified as Medical Center A. The attack revealed deficiencies in the medical center's security precautions and responses.

Engelman called on the Health Ministry to examine the findings of the penetration test to develop and implement recommendations for other medical institutions.

jns Jewish News Syndicate

Cyber-security czar: 'Those who attack Israeli citizens will pay'

Israeli security is focusing particularly on Iranian cyber attacks, said Israel National Cyber Directorate head Gaby Portnoy.

"Anyone who carries out cyberattacks against Israeli citizens must take into account the price he will pay," said Gaby Portnoy, director general of the Israel National Cyber Directorate, on Tuesday.

Speaking at Tel Aviv University's annual Cyber Week, Portnoy said: "In the past year, we have been working hard to develop our resilience and expand our capabilities to detect cyberattacks, raising our shields and expose malicious activities, specifically Iranian," said Portnoy, noting the vast majority of attacks are thwarted.

Portnoy mentioned specifically a cyberattack against the Technion-Israel Institute of Technology carried out by two groups associated with the Iranian Intelligence Ministry. The February incident took the form of a ransomware attack. The hackers demanded 80 bitcoins ($1.6 million) to call it off.

Portnoy added that Iran was also preying on civilian targets in "many countries like Turkey, Saudi Arabia, Egypt, Morocco, India, Oman, Bahrain, Kuwait and more."

The Israeli security community "knows the Iranian cyber activities inside out and is working to disrupt them in different ways," he said.

He called for tighter international cooperation against Iranian cyber activities and commended the United States "for imposing sanctions against two active cyber players in the [Iranian] Ministry of Intelligence and Security: Mojtaba Mostafavi and Farzin Karimi, who co-founded the Ravin Academy that trains hackers for malicious activities of the ministry."

Portnoy described some of the projects the Cyber Directorate has pursued over the past year, including partnering with the United Arab Emirates to build a "a multinational cyber collaboration platform."

He also noted the expansion of Israel's "Cyber Dome" project. Cyber Dome is a big-data, AI approach to cyber defense that Portnoy announced last year.

In January, Portnoy revealed that Israel's cyber defense authorities had repelled more than 1,000 attempted attacks that collectively had the potential to cripple the country's economy.

"As in the worlds of counterterrorism and spy games, the general public is mostly unaware of the attacks that have been stopped. Our job is to prevent those attacks that, if successful, would result in millions in damage to the economy and the country," he said.

VICTORIA ADVOCATE

Israel's int'l Cyber Week held in Tel Aviv

Israel's int'l Cyber Week held in Tel AvivDATELINE: June 28, 2023LENGTH: 00:01:21LOCATION: TEL AVIV, IsraelCATEGORY: TECHNOLOGYSHOTLIST:1. various of activities during the Cyber WeekSTORYLINE:Cyber Week, an annual international cybersecurity event, is being held at Tel Aviv University (TAU) in central Israel. The four-day event, which opened on Monday, is jointly organized by TAU, the Israeli National Cyber Directorate at the Prime Minister's Office, and the Ministry of Foreign Affairs, and is attended by more than 9,000 participants from over 80 countries and regions, according to a statement issued by TAU. Among the participants are experts, industry leaders, startup companies, investors, academics, diplomats, and government officials, it added. The event includes a conference, exhibitions, roundtables, panels, forums, workshops, and social events, offering knowledge exchange, methods, and ideas. Topics regarding cybersecurity in sectors of healthcare, cloud, economics and transportation, among others, will be discussed, according to the statement.Xinhua News Agency correspondents reporting from Tel Aviv, Israel.

GolfBusiness

Cyber Week 2023: Top cybersecurity experts gather to discuss latest trends

The annual cybersecurity event, hosted at Tel Aviv University, successfully concluded its 13th conference last month

BY DIVSHA BHAT

The 13th edition of Cyber Week, an annual cybersecurity event held at Tel Aviv University, concluded successfully, bringing together notable individuals from various sectors including industry, government, military, and academia.

Over 11,000 attendees from 99 countries participated at the event.

The event was jointly organised by the Blavatnik Interdisciplinary Cyber Research Center, 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 along with the Israel's Ministry of Economy and Ministry of Foreign Affairs.

Participants showcased the latest developments, challenges and opportunities in the field of cybersecurity.

Cyber Week featured speakers from around the world, including leading Israeli government officials such as Gaby Portnoy, director-general of the Israel National Cyber Directorate (INCD) and Ronen Bar, director of the Israel Security Agency (Shin Bet).

Maj. Gen. (Ret.) Prof Isaac Ben-Israel, recognised as the "father" of the Israeli Cyber industry, led the conference.

Global cyber officials also made significant contributions, including Kemba Eneas Walden, acting national cyber director in the Office of the National Cyber Director; Nathaniel C. Fick, ambassador at Large for Cyberspace and Digital Policy at the US Department of State; Minister Audrey Tang, Ministry of Digital Affairs Taiwan; Sami Khoury, head of the Canadian Centre for Cyber Security; Dr Mohamed Al Kuwaiti, head of Cybersecurity for the UAE Government; Craig Jones, cybercrime director at Interpol and Ann Dunkin, chief information officer of the US Department of Energy.

The conference also welcomed private sector leaders, such as Eric Doerr, VP of Engineering and Cloud Security at Google Cloud, Gil Shwed, founder and CEO of Check Point; Aviv Cohen, CMO of Pentera; Bret Arsenault, corporate vice president and chief information security officer of Microsoft; Udi Mokady, founder and executive chairman of CyberArk; Chris Roberts, CISO of Boom Supersonic; Lane Bess, CEO of Deep Instinct and others.

The conference took place amidst the backdrop of rapid AI development, the Ukrainian crisis and an alarming rise in cybercrime and cyber-related damages, which are projected to reach an annual cost of $10.5tn by 2025.

While concerns about the impact of AI across sectors, including cybersecurity, were discussed, speakers also expressed optimism about the transformative potential of this technology in addressing cybersecurity challenges.

Dr Al Kuwaiti discussed the importance of allies, detailing how Israel recently helped the UAE fend off a serious DDoS cyberattack. "Thank God for the Abraham Accords... Cybersecurity is an important aspect for us all. The UAE is going through great digital transformation across all sectors: aviation, education, healthcare, oil and gas, transportation. And as a matter of fact, we need to ensure a safe and secure digital transformation."

Dr Al Kuwaiti continued, describing how the UAE plugs into the startup nation's many companies to build and extend his country's "cyber dome" to defend against cyberattacks.

Read: Dr Al Kuwaiti leads UAE delegation at Cyber Week, highlighting UAE-Israel cyber alliance

Meanwhile Bar spoke at Cyber Week about how the Shin Bet is harnessing AI: "AI technology has been incorporated quite naturally into the Shin Bet's interdiction machine." He describes how "an alarming number of [cybersecurity cases] have a strong basis on the web – posts, inspiration, knowledge, or social groups.

The trend is clear. Traditional security organisations must adapt to the new situation, where any angry person with access to the Internet may become a threat.

Already today, with AI, we have identified a significant number of threats," he said. "Since we have understood we can't fight this war with sticks and stones, we recognise the threats but also see opportunities of using AI."

The importance of global collaborations was made clear. Jones commented on the legal challenges of cybersecurity: "When people say cybercrime is borderless, that really infuriates me because, as law enforcement officials, we are totally constricted by the countries and the legislation.

"To address the problem, Interpol has teams based around the world, providing "a framework for those countries and with secure platforms for communications."

Dunkin spoke on the importance of employing "a collective defense approach to cybersecurity." She said: "We must cooperate with like-minded international partners, focusing on innovation and cybersecurity capacity-building measures, cybersecurity for industrial control systems, the sharing of best practices, as well as workforce development strategies and training."

GolfBusiness

Dr Al Kuwaiti leads UAE delegation at Cyber Week, highlighting UAE-Israel cyber alliance

Cyber Week is an annual international cybersecurity event, hosted at Tel Aviv University in Israel for last 12 years
BY DIVSHA BHAT

Dr Mohamed Al Kuwaiti, head of Cybersecurity for the UAE Government, led a prominent UAE delegation of leading Emirati entities to the Cyber Week 2023 conference in Tel Aviv this week.

Cyber Week is an annual international cybersecurity event, hosted each year at Tel Aviv University in Israel for over last 12 years.

The participation from the UAE serves as a testament to the flourishing relation and strengthening bonds between the UAE and Israel in the realm of cybersecurity.

Dr Al Kuwaiti addressed the CyberWeek conference as a keynote speaker in the main plenary panel titled "Safeguarding the Nation: Cybersecurity Strategies for a Digital Age", along with Gaby Portnoy, director general of the Israel National Cyber Directorate and several top international government officials.

During the visit, the UAE delegation met with the central cyber stakeholders in the Israeli cyber ecosystem including investors, chief information security officers and top cyber experts.

They also visited cyber labs and R&D centres and startups to explore opportunities to deepen the ongoing

partnerships.

The visit provided valuable insights into the latest global trends in cybersecurity and allowed the participants to explore potential collaborations and bilateral investment opportunities.

Dr Al Kuwaiti, head of UAE Cyber Security Council said: "Cybersecurity is a shared responsibility that can never be addressed by one person, organiSation or country alone.

Instead, it requires mutual collaboration between the private and public sectors. Partnership with the industry and academia is critical as it brings all the stakeholders of the digital ecosystem together with a common vision. Our goal is to spread the cyber security culture. The end result will be a more secure, more resilient digital future, not only for the UAE but for our partners and friends."

Amir Hayek, ambassador of Israel to the UAE said: "This delegation, led by Dr Mohamed Al Kuwaiti, represents the ongoing collaboration between Israel and the UAE in the cybersecurity domain, as both nations recognise the critical importance of a secure and resilient digital infrastructure.

Israel remains committed to nurturing these relationships and promoting cross-border partnerships in cybersecurity and beyond."

EliteCISOs, Cyber Together MoU signed at Cyber Week

On the sidelines of the Cyber Week conference, the UAE-based EliteCISOs, a global cybersecurity community, signed a Memorandum of Understanding with the Israel-based Cyber Together, an Israeli NGO, to expand this global community to Israel.

The MOU marks the beginning of a strategic partnership aimed at fostering cooperation in the field of cybersecurity between key professionals in both countries.

The signing event was held in the presence of Dr Al Kuwaiti and Oded Joseph, deputy director general, head of Middle East Division in the Ministry of Foreign Affairs, Israel.

Joseph stated: "Israel is fully committed to fostering collaborations and partnerships with the UAE between the various ecosystems of innovation of our nations.

This MoU, a strategic partnership between two leading cyber security stakeholders, further strengthens our relations and represents the shared benefits of the Abraham Accords beyond the relationship between governments to partnerships between organisations and people."

Under the terms of the MOU, EliteCISOs and Cyber Together will collaborate on various initiatives including knowledge-sharing, joint training and workshops to enhance cybersecurity capabilities, promote the development of a cybersecurity workforce and address emerging threats in both the UAE and Israel.

The relationship between EliteCISOs and Cyber Together was initiated and fostered by the Consulate-General of Israel in Dubai as part of its wider effort to establish new cyber-based partnerships between entities in the two countries.

L'USINE DIGITALE

A Tel-Aviv, la cybersécurité en ordre de bataille face aux défis posés par l'intelligence artificielle

Avec plus de 470 cyber start-up actives, Israël se classe au second rang mondial des clusters de cybersécurité. Lors de la Cyber Week, grand-messe du secteur qui vient de se dérouler à l'Université de Tel-Aviv, ses représentants ont expliqué pourquoi l'IA représentait autant une menace qu'une opportunité. Visite guidée dans quelques hauts lieux de cet écosystème atypique : de Petah Tikva, où réside le champion de la protections des accès CyberArk, à Tel-Aviv dans les locaux de la cyber pépite du cloud Wiz, en passant par le CyberSpark de Beer Sheva qui inspiré le campus cyber de la Défense.

Cette année encore, la Cyber Week, grand évènement de la cybersécurité israélienne, qui a réuni la semaine dernière près de 11 000 participants venus de 100 pays, a affiché complet avec son lot d'annonces fracassantes tant pour les visiteurs du secteur privé que pour l'univers de la recherche ou le monde militaire.

Ils ont évoqué les défis posés par la cybercriminalité, qui devraient coûter 10 500 milliards de dollars par an d'ici 2025, et ont encouragé la collaboration pour lutter contre cette menace croissante. Parmi les têtes d'affiche de ce rassemblement atypique d'experts en cybersécurité, de leaders de l'industrie, de start-up, d'investisseurs, d'universitaires, de diplomates autres représentants gouvernementaux, figurait notamment le chef de la cybersécurité des Émirats arabes unis, Mohamed Al-Kuwaiti.

Lors du coup d'envoi de la 13ème Cyber Week organisée par le Blavatnik Interdisciplinary Cyber Research Center de l'Université de Tel-Aviv, ce dernier a remercié Israël et son cyber système national l'avoir aidé "à repousser une cyberattaque par déni de service, de type DDoS", ainsi que pour l'assistance apportée par l'État hébreu aux Émirats dans la mise en place du "cyber dôme de fer". "La grande start-up nation (Israël) et ses nombreuses entreprises nous ont aidés et nous aident encore à construire un cyber dôme de fer ou à améliorer celui existant", a-t-il indiqué.

Le responsable de la cybersécurité des EAU a ensuite présenté à Tel-Aviv le projet Crystal Ball : une plateforme numérique destinée à détecter et repousser les pirates dont Microsoft, la firme israélienne Rafael Advanced Defense Systems et CPX, basé à Abu Dhabi, fournissent l'épine dorsale technologique. Plusieurs pays participent à cette initiative censée favoriser le partage d'informations pour lutter contre la piraterie informatique et les rançongiciels. "Les cybermenaces ne font pas de distinction entre les nations, ne font pas de distinction entre les entités ou les personnes", a indiqué Al Kuwaiti. "C'est pourquoi nous devons nous unir contre ces menaces, et la boule de cristal que nous visons pour toute la communauté, sera le premier pas vers cela."

Lors de la présentation de Crystal Ball, le PDG de Microsoft Israël, Alon Haimovich, a souligné que cette réponse était nécessaire pour lutter contre la sophistication croissante des pirates. Elle offrira "la puissance, les capacités et les connaissances nécessaires pour lutter contre les attaques de rançon en temps réel avec une coopération continue, pratique et de haute qualité", a-t-il déclaré dans un communiqué de presse du gouvernement israélien.

La plateforme est conçue par Microsoft dans le cadre de l'International Counter Ransomware Initiative (CRI), une entreprise mondiale dirigée par la Maison Blanche qui comprend 15 États membres, dont les Émirats arabes unis, l'Allemagne, la Grande-Bretagne, Singapour, ainsi que l'Organisation internationale de police criminelle (Interpol).

Dôme de fer cybernétique

Trois ans après la normalisation des relations diplomatiques entre les Émirats arabes unis et Israël dans le cadre des accords d'Abraham, force est de constater que les liens commerciaux et stratégiques entre les pays se sont renforcés, selon Al Kuwaiti. La connexion avec les entreprises technologiques israéliennes "a été particulièrement utile dans la transition de son pays vers une économie numérique".

"Nous sommes confrontés à des défis communs dans le domaine du cyber, a renchéri le responsable du cyber système national israélien, Gaby Portnoy. La surface d'attaque s'étend avec les nouvelles technologies et la motivation croissante des cyber assaillants. Nous devons relever les défis avec nos partenaires, utiliser les connaissances que nous avons acquises et les nouvelles technologies pour une protection meilleure et plus rapide."

Le projet a initialement été dévoilé lors d'une rencontre survenue en marge de la Cyber Week, en présence du Premier ministre israélien Benyamin Netanyahu au siège de l'Agence de sécurité israélienne (ISA ou "Shin Bet"), dont le directeur, Ronen Bar, a évoqué les enjeux liés à l'utilisation croissante de l'intelligence artificielle. "L'ISA et l'IA ont un point commun : nous gagnons tous les deux notre vie en recherchant des modèles et des anomalies", a souligné ce responsable, faisant remarquer que l'agence avait également développé son propre outil d'IA générative qui peut être utilisé comme ChatGPT d'OpenAI.

Une autre innovation de l'IA testée par l'ISA est un système de sécurité aéroportuaire qui, selon lui, "changerait radicalement" le processus de contrôle avant l'enregistrement des vols. "Peut-être qu'un jour, a-t-il glissé lors de la conférence de Tel Aviv, nous abandonnerons la question favorite traditionnelle pour vous tous : avez-vous fait vos bagages tout seul ?"

Ronen Bar a par ailleurs annoncé que l'ISA mettait en place un incubateur technologique pour aider les start-up à développer des produits d'IA générative afin de répondre aux besoins en sécurité et renseignement. L'IA aidera l'agence à hiérarchiser les informations, à renforcer les capacités de renseignement en identifiant les modèles et les écarts par rapport aux modèles ; à devenir un outil dans le processus décisionnel et à aider à prévoir les tendances et la probabilité de leur réalisation. Pour l'agence, l'IA générative sera un "partenaire" à la table de prise de décision, a conclu Ronen Bar, mais pas un "décideur".

Durant la Cyber Week, un ancien responsable du Pentagone a en outre interpellé les gouvernements et les entreprises qui ne prêtaient pas suffisamment attention aux dangers potentiels de l'IA. "Je pense qu'Israël devrait être très préoccupé par les algorithmes que l'Iran pourrait essayer de développer ou d'acquérir à l'étranger", a déclaré Ezra Cohen, ex-sous-secrétaire à la Défense par intérim pour le renseignement et la sécurité, et désormais vice-président de la stratégie d'entreprise chez Oracle Corp. "Maintenant, je ne dis pas que nous devrions traiter l'IA aujourd'hui comme une arme nucléaire ou quoi que ce soit de ce genre, a-t-il ajouté, mais certaines procédures devraient être mises en place."

Logiciels malveillants alimentés par l'IA : la préoccupation n°1

Les grands noms de l'écosystème israélien, qui avec 470 cyber start-up actives, se classe au second rang mondial des clusters de cybersécurité, ont pour leur part relayé d'autres préoccupations. Plaçant au cœur des débats, le sujet de l'IA, perçue tant comme une source de menace que de nouvelles opportunités, ils n'ont pas manqué de mettre en avant l'efficacité de leurs solutions, études de cas à l'appui. Lors du panel "De l'attaque à la défense : utiliser l'IA pour combattre la cybercriminalité financière basée sur l'IA", Mark Gazit, le patron de ThetaRay (en photo ci-dessous), a expliqué comment sa solution permettait aux banques de mieux servir leurs clients, de repérer de nouvelles opportunités et d'augmenter leurs revenus, tout en gardant une longueur d'avance sur les criminels.

Fondée en 2012 par deux mathématiciens, Amir Averbuch de l'Université de Tel-Aviv, et Ronald Coifman, de l'Université de Yale, la compagnie basée près de Tel-Aviv, s'appuie sur plus de dix années de recherche dans le domaine des algorithmes capables d'analyser des masses de données et de détecter en temps réel l'occurrence d'anomalies. A l'actif de la plateforme d'IA "profonde" de la société : l'identification d'un réseau choquant de trafic d'êtres humains en Ukraine, utilisant une clinique de santé comme façade.

"Notre technologie a fourni une visibilité sur les paiements internationaux, aidant à démanteler le réseau criminel qui opérait dans plusieurs pays, y compris les États-Unis, l'UE et les territoires offshore", a indiqué Mark Gazit. ThetaRay a également signalé des activités suspectes impliquant une succursale locale en Europe de l'Est qui utilisait des comptes prétendant aider des enfants. En identifiant rapidement ces anomalies, la firme espère

avoir “évité de nouveaux dommages et protégé des vies innocentes”.

Autre intervention remarquée, celle d’Udi Mokady, fondateur et président exécutif de CyberArk, la deuxième entreprise de cybersécurité du pays derrière Check Point, l’inventeur du pare-feu informatique. Selon l’enquête annuelle réalisée dans seize pays (dont Israël) par ce spécialiste du contrôle des accès informatiques, “93 % des professionnels de la sécurité interrogés s’attendent à ce que les menaces basées sur l’IA affectent leur organisation en 2023, les logiciels malveillants alimentés par l’IA étant cités comme la préoccupation n°1.”

Lors d’un entretien accordé à L’Usine Digitale, en marge de la Cyber Week, dans l’immeuble moderne entièrement occupé par son entreprise, situé à Petah Tikva (en banlieue de Tel-Aviv), Udi Mokady s’est toutefois montré plutôt rassurant. “Les systèmes deviennent de plus en plus intelligents et l’IA permet aux cyber-assaillants de mettre en place des fraudes très sophistiquées, y compris via l’écriture des codes, confie ce dirigeant. Mais l’IA s’avère également utile pour notre secteur. Et les organisations n’auront pas d’autre choix que de se montrer plus intelligentes : tant dans la gestion des accès de leurs collaborateurs que dans le contrôle des identités des machines.”

Tout juste rentré d’un grand évènement organisé pour sa clientèle à Paris sur le campus cyber de la Défense (dont CyberArk est l’un des sponsors), Udi Mokady ne s’inquiète pas non plus outre mesure de la crise qui secoue la tech israélienne, qui a vu ses investissements chuter de 68% (selon le Start-up Nation Policy Institute) au premier semestre 2023, et annoncé des licenciements en série. “L’entreprise que j’ai fondée en 1999, n’a jamais été en sureffectif, a-t-il fait valoir, et comme le sujet de la sécurité des identités n’est pas négociable, on résiste bien.”

Avec ses solutions SaaS visant à protéger dirigeants et informaticiens qui administrent les réseaux internes des entreprises, la firme compte 8 000 clients et 2800 salariés dans le monde, dont une cinquantaine de collaborateurs dans l’Hexagone, “soit deux fois plus qu’il y a six ou sept ans.”

Sécuriser l’IA sur le cloud

Même son de cloche optimiste dans les locaux de Wiz, la cyber pépite du cloud, juchée au 23ème étage d’une tour du cœur de Tel-Aviv. Ex-Microsoft Defender, Alon Schindel, son directeur Data & Threat Research, qui nous accueille sur les lieux, ne regrette pas d’avoir rejoint cette nouvelle licorne fondée début 2020 par quatre anciennes recrues de l’unité 8200 des services de renseignements de l’armée israélienne (dont est aussi issu le patron de CyberArk). Après avoir créé la firme Adallom - cédée en 2015 pour 350 millions de dollars à Microsoft, le quatuor qui a officié au sein du groupe Cloud security de Microsoft Azure, s’est mis en tête de résoudre un problème “assez global” : la sécurisation de l’infrastructure du cloud.

La société, dont le siège social est basé à New York et qui a atteint en un temps record (18 mois après sa création) le cap des 100 millions de dollars de revenus annuels, s’est rapidement imposée avec une offre unique : une “solution de visibilité cloud pour la sécurité des entreprises, fournissant aux clients du cloud une évaluation contextuelle des risques afin de permettre une réduction spectaculaire des alertes de sécurité, un plan d’action clair et une protection à grande échelle”.

Ce positionnement lui a valu en juin 2021 de clôturer une levée de fonds de série B de 120 millions de dollars auprès de Salesforce Ventures et Blackstone, à laquelle a également participé le patron du groupe LVMH, Bernard Arnault, via sa société de capital-risque, Aglaé Ventures, aux côtés du milliardaire américain Howard Schultz, l’ex patron historique de Starbucks. Autre titre de gloire de la société qui a levé 300 millions de dollars en février dernier, et dont 35% des clients se trouvent dans le classement Fortune 100 : la découverte d’une faille de sécurité majeure affectant Bing.

Ses chercheurs en sécurité informatique ont dévoilé que non seulement celle-ci permettait de modifier en quelques clics les résultats d’une recherche effectuée sur le moteur de Microsoft, mais qu’elle permettait aussi de mettre la main sur des données sensibles de ses utilisateurs.

“Aujourd’hui les ingénieurs utilisent davantage Wiz que les équipes dédiées à la sécurité informatique pour les données sensibles, se félicite Alon Schindel. Ceux qui fabriquent les data services travaillent souvent très vite. Et notre objectif est d’assurer le maximum de fluidité entre toutes les parties.” L’un des prochains enjeux pour ce nouveau cyber champion israélien consistera aussi à sécuriser l’IA sur le cloud. Et ce, alors que ses clients devront apprendre à se servir des LLM (Large Language Models) et des données pour expliquer ce qui se passe lors d’une menace cybernétique...

ISRAELDEFENSE

Israel's Cyber Chief Says Iran Will "Pay a Price" If Attacks Continue

Speaking At Tel Aviv University's Cyber Week, Portnoy said that "In the past year, we have been working hard to develop our resilience and expand our capabilities to detect cyberattacks"
Mandi Kogosowski

Gaby Portnoy, Director General of Israel National Cyber Directorate, discussed Iran's and Hezbollah's offensive cyber activities against Israel at Tel Aviv University's Cyber Week, saying that "Anyone who carries out cyberattacks against Israeli citizens must take into account the price he will pay for it."

Speaking earlier this morning in the plenary, Portnoy said that "In the past year, we have been working hard to develop our resilience and expand our capabilities to detect cyberattacks, raising our shields and expose malicious activities, specifically Iranian." He added that the vast majority of attacks are thwarted.

During his presentation, Portnoy mentioned the cyberattack against the Technion carried out by MuddyWater in collaboration with Darkbit – two attack groups associated with the Iranian Ministry of Intelligence. "They are also attacking civilian targets in many countries like Turkey, Saudi Arabia, Egypt, Morocco, India, Oman, Bahrain, Kuwait, and more," he said.

"The Israeli defense community knows the Iranian cyber activities inside out and is working to disrupt them in different ways. The people of the Iranian Ministry of Intelligence, and from IRGC and Hezbollah, who are involved in cyber operations against Israel know very well what I am talking about."

Portnoy called on the international community to work tightly together, in order to stop malicious cyber actors. He described a joint project with the UAE, which includes developing "a multinational cyber collaboration platform for cyber investigation and knowledge building...This platform will serve almost 40 countries and organizations that are part of the Counter Ransomware Initiative led by the White House."

Discussing the much-anticipated "Cyber Dome" – a system based on AI and big data, intended to provide an overall approach to proactive defense

"Our experts are working together with many partners to design, build and expand our Cyber Dome, as part of a national and multinational resilience effort. Also, we are designing sectorial on-cloud SOCs with Google and building a portal for better communication with our government and private organizations," Portnoy said.

ISRAELDEFENSE

Former Senior Pentagon Official Says Israel Must Maintain AI Edge

Speaking in Tel Aviv, Ezra Cohen said he believes that "automation and AI will really reduce and have great potential in reducing civilian harm"

In a recent interview during Tel Aviv University's Cyber Week conference, former US Acting Undersecretary of Defense for Intelligence and Security, Ezra Cohen, shared his perspectives on the utilization of artificial intelligence (AI) in military applications.

Addressing the potential of AI in reducing civilian casualties and maintaining Israel's advantage over adversaries, Cohen – who is now VP for Corporate Strategy at Oracle Corp., highlighted the significance of technological advancements and ethical considerations in the field.

Regarding the role of AI in minimizing civilian harm, Cohen emphasized its potential in kinetic actions.

"I think at the more tactical level, there is a lot of talk about killer drones basically going all over autonomously killing people," he explained at the Cyber Week conference. However, Cohen offered a different perspective,

stating, "The reality is that I actually see that automation and AI will really reduce and have great potential in reducing civilian harm."

With advanced AI algorithms and computer vision capabilities, drones equipped with AI can surpass human abilities in identifying civilians in conflict zones, thereby mitigating harm to non-combatants.

Moreover, Cohen highlighted the need for Israel to maintain its edge over adversaries, particularly in the field of AI, as discussed at the Cyber Week conference.

"The adversaries are investing in AI. In Israel, the issue is always maintaining an edge, and I think it is essential, certainly for the US, which depends on Israel in the Middle East," he stated. Recognizing the strategic importance of AI, Cohen underscored the necessity for Israel to retain superiority in AI technologies, ensuring national security interests and close collaboration with the United States.

The discussion further delved into the delicate balance between AI-driven autonomy and the role of human decision-making in military operations. While recognizing the potential of autonomous systems, Cohen stressed the importance of keeping humans in the loop.

"I think at least in the US, there is still a heavy weight to keep some humans in the loop, and the US DoD put AI guidelines for use in military purposes earlier this year," he stated. Highlighting the risk associated with AI hallucination, where misinterpretation of signals or misjudgments could lead to significant consequences, Cohen urged caution in relinquishing human control entirely.

As AI continues to shape defense and security landscapes, Cohen emphasized the need for robust policies and procedures to prevent the misuse of AI technology. Drawing parallels with nuclear weapons, he noted, "There is a point when technology crosses a threshold where it needs to be more controlled." While acknowledging the benefits AI offers, he emphasized the importance of striking a balance between harnessing its potential and ensuring responsible deployment.

eSecurity Planet

Mockingjay Attack Evades EDR Tools with Code Injection Technique

Kaye Timonera

Security researchers have identified a new sophisticated hacking technique, dubbed "Mockingjay," that can bypass enterprise detection and response (EDR) tools by injecting malicious code into trusted memory space. This stealthy approach allows attackers to operate undetected within an organization's network for extended periods.

The attack technique — identified by researchers at Security Joes — is a challenge to EDR vendors and security teams alike.

"To effectively counteract such attacks, security solutions need to employ a comprehensive and proactive approach that goes beyond static monitoring of specific DLLs or system calls," the researchers wrote. "Behavioral analysis, anomaly detection, and machine learning techniques can enhance the ability to identify process injection techniques and detect malicious activities within the memory space of trusted processes."

The Mockingjay Attack Explained

The Mockingjay attack targets trusted and legitimate processes running on the system and avoids or minimizes use of Windows APIs that EDR tools commonly associate with injection attacks. By secretly injecting malicious code into the memory space of the trusted process, Mockingjay hides its activities within a seemingly harmless process.

EDR tools typically monitor Windows APIs within the memory space of processes to detect injection attacks, so the researchers set about trying to find other methods to dynamically execute code within the memory space of Windows processes without relying on the monitored Windows APIs.

They detailed two such attack techniques in their blog post.

They explored trusted Windows libraries that contain sections with default protections set as RWX (Read-Write-Execute). "By misusing these libraries, we were able to successfully inject code into various processes and eliminate the need to execute several Windows APIs usually monitored by security solutions," they wrote. "This approach reduces the likelihood of detection by defense software, as our application does not directly invoke Windows APIs typically associated with process injection techniques. The injection is executed without space allocation, setting permissions or even starting a thread. The uniqueness of this technique is that it requires a vulnerable DLL and copying code to the right section."

Both attack techniques involve processes located within Visual Studio 2022 Community. The first is the DLL msys-2.0.dll, and the second attack technique targets the ssh.exe process located within the Visual Studio 2022 Community directory.

The msys-2.0 DLL contains a default RWX section that could potentially be exploited to load malicious code,

the Security Joes researchers said. The report goes into great detail on the attack technique, which they summarized in six steps:

Custom application loads vulnerable DLL using LoadLibraryW

Location of the RWX section is resolved using the base address of the DLL and the offset of section

A clean copy of NTDLL.DLL is loaded from the disk, and the system call numbers for the desired syscalls are obtained

The addresses of the test instructions after the jmp added by the EDR are retrieved from the NTDLL.DLL in-memory copy (hooked by the EDR)

Using the addresses of the test instructions and the syscall numbers, the researchers assemble their stubs in the RWX area of the vulnerable DLL

When the stub is executed, it prepares the syscall number in the EAX register, as usual, and immediately jumps to the address of the corresponding test instruction for the chosen system call, bypassing the EDR verification step

Second EDR Attack Detailed

In the process of their work, the researchers noticed that the msys-2.0.dll library is "commonly utilized by applications that require POSIX emulation, such as GNU utilities or applications not originally designed for the Windows environment. We found relevant binaries with these characteristics within the Visual Studio 2022 Community subdirectory."

For their proof of concept, they chose the ssh.exe process located within the Visual Studio 2022 Community directory as the payload target. "To accomplish this, we initiated the ssh.exe process as a child process of our custom application using the Windows API CreateProcessW," they wrote, summarizing the attack technique as follows:

Custom application is executed

Trusted application (ssh.exe) using DLL msys-2.0.dll is launched as a child process

Custom application opens a handle to the target process (ssh.exe)

Code to be injected is copied into the RWX section of msys-2.0.dll

Trusted application executes the injected code during its normal execution flow

Additional DLL MyLibrary.dll is loaded by the shellcode injected in the RWX section

Back connect shell session is established

"The uniqueness of this technique lies in the fact that there is no need to allocate memory, set permissions or create a new thread within the target process to initiate the execution of our injected code," they wrote. "This differentiation sets this strategy apart from other existing techniques and makes it challenging for endpoint detection and response (EDR) systems to detect this method."

How to Defend Against a Mockingjay Attack

EDR systems with integrated behavioral analytics can stop a Mockingjay attack by broadening the scope of their monitoring to cover trusted processes. Such detection techniques can identify code injection and unauthorized changes by establishing baseline behavior patterns and conducting memory integrity checks. EDR technologies can improve their capacity to recognize and block Mockingjay attacks through contextual analysis and the application of machine learning methods that can detect anomalous patterns.

For security teams, Mockingjay is yet another argument for defense-in-depth; if one security tool misses an attack, a second one could potentially limit the damage.

U.S. Chamber of Commerce

U.S. Chamber of Commerce Business Delegation Leads at Israel's Cyber Week

From June 25-30, the U.S. Chamber led its third annual business mission to Israel's Cyber Week.

This global conference brought together 11,000 international cybersecurity experts and policymakers, including 400 speakers representing 100 countries from the U.S., Europe, the Middle East, and Asia, for discussions about cyber policy and technology issues and to build alliances to strengthen our collective cyber defense.

Why Israel? The US-Israel cyber relationship—public and private—is a global model in that we have a common risk-based approach to regulation, strong public-private dialogue, and active bilateral R&D relationships. Around 20% of global investment into cybersecurity start-up companies goes to Israeli firms. This is a boon for U.S. companies looking for cyber solutions. Throughout our visit, we worked closely with our partners in Israel to connect our delegates with new technologies solutions and new deals were inked from this fruitful collaboration.

ENGAGEMENT WITH ISRAEL'S CYBER ECOSYSTEM

We visited Be'er Sheva, known as Israel's "cyber capital," where we toured Israel's National Cyber Emergency Response Team (CERT), cyber innovation laboratories focused on intelligent transportation systems and industrial control systems, and the IDF School of Computer Science also known as "Basmach." We discussed opportunities to enhance collaboration with Israel's National Cyber Directorate (INCD) in areas such as health and transportation, how we might drive a global private-private coalition to promote "security by design," and how the Abraham Accords could promote regional cyber cooperation.

INTERNATIONAL CYBER ENGAGEMENT

The U.S. Chamber convened policy roundtables with influential cyber leaders from nearly a dozen cybersecurity agencies around the world, including the U.K., UAE, Singapore, Israel, Czech Republic, Sweden, Spain, and Canada. These discussions focused on national cyber strategies and emphasized the importance of addressing the harmful impact of digital sovereignty on cybersecurity and digital commerce. For our policy priorities, see here.

U.S.-ISRAEL COMMERCIAL POLICY PRIORITIES

The delegation and members of our US-Israel Business Council met with senior Israeli officials—including Tzachi Hanegbi, National Security Advisor, Gaby Portnoy, Director General, Israel National Cyber Directorate, and others from the Ministries of Health, Economy & Industry, and Finance—to discuss priorities trade, innovation, and investment, including ongoing private sector engagement in the upcoming U.S.-Israel Strategic High Level Dialogue on Technology.

U.S. ISRAEL DIGITAL FORUM

Hosted at Microsoft's campus in Herzliya, the U.S. Chamber convened a forum focused on digital policy issues that included representatives from Israel's Ministries of Economy & Industry, Justice, and Privacy Protection Authority to discuss the regulatory and legal frameworks in Israel for emerging digital technologies. Participants discussed the need to balance the opportunities for joint innovation with strong privacy and cyber protections. Israel is considering joining the Cross Border Privacy Rules (CBPR) Forum and will seek public comment when a revision of the national privacy law is released. A special thank you to the Israel Hi-Tech Association, the Israel Manufacturers Association, and AmCham Israel, for their support in organizing the program.

CYBER WEEK CONFERENCE

Members of our delegation participated in or led numerous conference programs, including Israel Healthcare Cybersecurity Summit, Cybersecurity Regulation in the Age of A.I., A.I. & Cyber, Regulating Cyber Surveillance - New Public/Private Partnership, Securing the ICT Supply Chain from Cybersecurity Threats, Embracing the Quantum Computing Revolution: Unleashing the Opportunities for Cybersecurity, CISO Roundtable, The BOMs are coming, Emerging Threats to Critical Infrastructure, and the Intelligent Transportation Systems Cybersecurity Summit. Members of the delegation benefited from the unique opportunities and collaboration that the U.S. Chamber has with Tel Aviv University to provide thought leadership and expertise on the part of their organizations to a global audience. As evidenced by the quality of the audience questions, worldwide community members are informed and influenced by the U.S. approach to cybersecurity policy regulations.

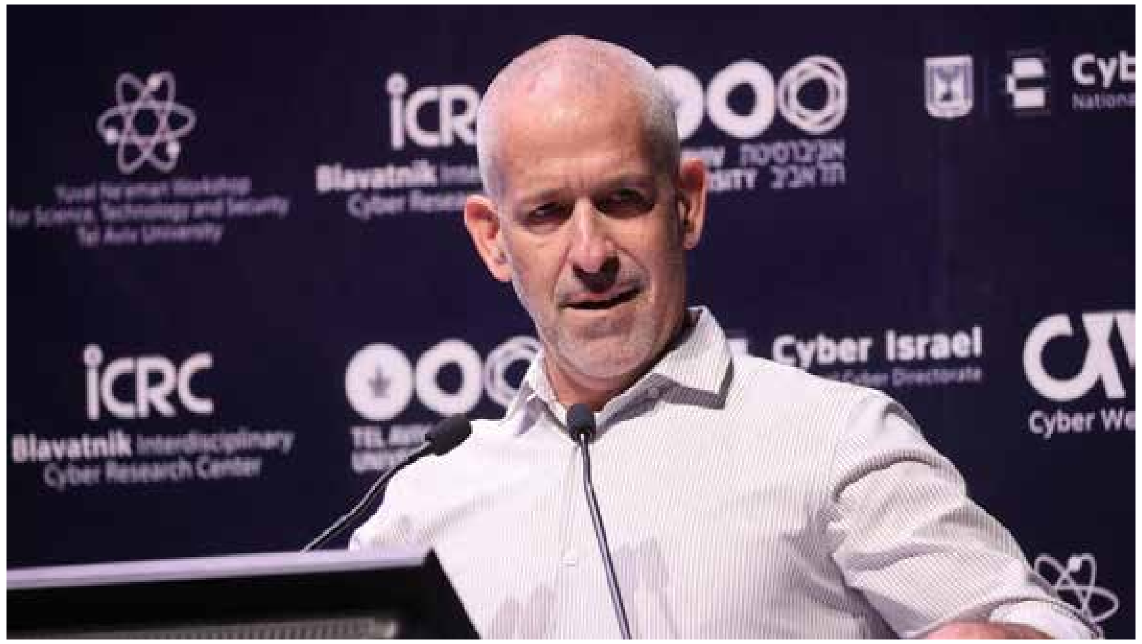
GLOBAL CYBER CABINET GALA DINNER

With special thanks to Honeywell, Quantinuum, Waterfall Security, and Microsoft, the U.S. Chamber hosted an unforgettable gala dinner, which brought together 150 attendees, including esteemed guests such as Kemba Walden, Acting National Cyber Director at the White House, Nate Fick, Ambassador-at-Large for Cyberspace and Digital Policy, and officials from Commerce, DHS, FBI, and DOE. In their keynote remarks, Director General Portnoy, Matt Bohne from Honeywell, and Andrew Ginter from Waterfall Security stressed the importance of public-private partnerships, international collaboration, and common, technical, risk-based approaches to cybersecurity policy.

allisraelnews

Israel uses AI to identify, prevent terror threats, says Israeli security chief

Bar talks about new kind of terrorist that is 'born from the smartphone camera, not inside a mosque'



Shin Bet Chief Ronen Bar, the director of the Israel Security Agency (ISA), confirmed that Israel uses artificial intelligence (AI) technology to identify and prevent threats of terrorism.

"The AI technology was assimilated into the Shin Bet's countermeasures machine naturally. We identified a significant number of threats using AI," Bar said on Tuesday, during the annual International Cyber Week conference hosted by Tel Aviv University.

"In order to make sure that AI will lead to evolution and not revolution, we will need cooperation and openness between the technology giants and the security agencies," he added.

Bar also said that traditional security organizations must adapt to modern times.

"Traditional security organizations are required to adapt to the new situation, where any angry person with access to the Internet may become a threat," he said, stressing that it is impossible to "win this war with sticks and stones."

Bar specifically mentioned the Lion's Den terrorist group as an example, saying that it represents a new kind of terrorist that is "born from the smartphone camera, not inside a mosque."

"We are in the depths of the network and see very well what is happening in it: espionage, terrorism, incitement, and foreign influence. The network, like the terrorists' nests in Jenin and the terror tunnels in Gaza, is not a safe space for our enemies," Bar said.

"The Iron Dome that the Shin Bet is developing in cyberspace is already taking its first steps, the array of alliances is emerging and it has already come into action. We are already cooperating with a number of significant countries in the field and we see the global cyber iron dome beginning to take shape," Bar noted.

THE AUSTRALIAN jewishnews

Aussies heading to Israel Cyber Week

Israel Cyber Week is a premier global conference that brings together more than 10,000 attendees from over 80 countries

Eighteen cybersecurity professionals from Australia and New Zealand are heading off to Tel Aviv for Israel Cyber Week.

Israel Cyber Week, a premier global conference that brings together more than 10,000 attendees from over 80 countries, providing a platform to showcase the latest advancements in the rapidly-evolving field of cybersecurity, takes place from June 26 to June 29, 2023, in Tel Aviv.

Distinguished speakers at the event will include Gaby Portnoy, Director General of the Israel National Cyber Directorate; Ivan Bartos, Deputy Prime Minister for Digitlisation of the Czech Republic; Craig Jones, Cybercrime Director at INTERPOL; and Iftah Gideoni, Former CTO of Forter, currently residing in Australia.

The Australia/New Zealand business delegation has been organised by the Israel Trade and Economic Commission in Sydney in partnership with the Trans-Tasman Business Circle.

Last year, the Australian and New Zealand Delegation to Israel Cyber Week made history as the first-ever in-person delegation from the region. This year, the delegation aims to build upon that achievement and foster deeper collaboration and knowledge sharing.

The Australian Ambassador to Israel, Ralph King, will address the delegation, providing valuable insights and strengthening ties between the two nations.

Additionally, the delegation will visit Lumir Ventures, Josh Liberman's Israel investment Fund in Melbourne, and prominent Israeli cybersecurity companies such as Checkpoint, Orca, Sentra, and Sygnia. These visits are designed to excite the delegates about the dynamic Israeli tech scene and its potential for future partnerships.

The itinerary includes a visit to Beer Sheva following a tour of the Anzac Museum and Cemetery. The delegates will also have the opportunity to explore the cultural and historical wonders of Jerusalem, the Dead Sea, and Masada.

Jeremy Ungar, who is responsible for cybersecurity at the Israel Trade and Economic Commission, expressed his enthusiasm for Israel Cyber Week.

"Israel Cyber Week has firmly established itself as a must-attend event on our annual calendar. With Australia now being the most-hacked country in the world, it is crucial for business leaders from all industries to understand the cybersecurity ecosystem and find better ways to protect their companies," he said.

"Israel Cyber Week offers an unparalleled opportunity to learn from the best in the field. This delegation not only showcases the expertise of our region but also provides a unique learning experience to explore the finest aspects of Israeli technology."

The Israel Trade and Economic Commission promotes trade and investment opportunities between Israel and international markets. The Trans-Tasman Business Circle is an influential and collaborative organisation that facilitates connections and knowledge sharing between Australian and New Zealand business leaders.

Israel developing cyber iron dome system to tackle threats using AI

Tel Aviv: Ronen Bar, the head of Israeli security agency Shin Bet, said Tuesday that Tel Aviv was developing the "global cyber iron dome" system in cooperation with a number of countries to identify and tackle threats using artificial intelligence (AI).

"The Iron Dome that the Shin Bet is developing in cyberspace is already taking its first steps, the array of alliances is emerging and it has already come into action. We are already cooperating with a number of significant countries in the field and we see the global cyber iron dome beginning to take shape," the i24NEWS broadcaster quoted Bar as telling the annual International Cyber Week conference hosted by Tel Aviv University.

Bar said that the agency was effectively using AI technology to prevent terror threats, adding that "the AI technology was assimilated into the Shin Bet's countermeasures machine naturally."

"We identified a significant number of threats using AI ... In order to make sure that AI will lead to evolution and not revolution, we will need cooperation and openness between the technology giants and the security agencies," he said.

The chief added that the agency realized it was impossible to "win this war with sticks and stones."

"We are in the depths of the network and see very well what is happening in it: espionage, terrorism, incitement, and foreign influence. The network, like the terrorists' nests in Jenin and the terror tunnels in Gaza, is not a safe space for our enemies," he said.

Iron Dome is an Israeli air defense system developed by Rafael Advanced Defense Systems and Israel Aerospace Industries and deployed in 2011. The system is capable of intercepting and destroying short-range rockets and artillery shells in a radius of up to 43 miles.

Israel Missile Defense Organization Director Moshe Patel said in late May that Iron Dome has carried out more than 5,000 successful interceptions of incoming short-range missile attacks since the system was deployed.

The Weekly Circuit

The head of cybersecurity for the United Arab Emirates, Mohamed Al Kuwaiti, leads an international cast of government officials, corporate executives and investors gathering today on the campus of Tel Aviv University for its annual CyberWeek conference. The early summer event will also feature Christopher Lukas, the chief information security officer for Chevron, which co-owns a Mediterranean gas field off the coast of Israel with Abu Dhabi's Mubadala sovereign wealth fund.

CyberWeek will kick off with addresses by the director of Israel's Shin Bet security agency, Ronen Bar, and chief of the Israel National Cyber Directorate, Gaby Portnoy. Coming from overseas are the acting U.S. national cyber director, Kemba Eneas Walden; Taiwan's digital affairs minister, Audrey Tang; the head of the Canadian Centre for Cyber Security, Sami Khoury; and Interpol's cybercrime director, Craig Jones.

Also on the roster are the chief information security officer for Microsoft, Bret Arsenault; the NFL's chief information security officer, Tomás Maldonado; Check Point Software Technologies CEO Gil Shwed; CyberArk Executive Chairman Udi Mokady; and the head of intelligence for Crowdstrike, Adam Myers.

At the Paris Air Show last week, Saudi Arabia emerged with a series of multibillion-dollar aircraft deals and showed off its newest carrier, Riyadh Air. Among the orders placed were 30 Airbus A320neo aircraft by the budget airline Flynas and 30 Boeing jets by its flag carrier Saudia. The kingdom intends to serve as a global logistics hub by doubling its air cargo capacity to 4.5 million tons by 2030, according to a statement by the Saudi General Authority of Civil Aviation.

Israel Aerospace Industries used the French exposition to unveil its new $1 billion Oron stealth jet. The aircraft is designed primarily for intelligence-gathering, with one-third of its weight taken up by dozens of high-performance computers and eight stations for intelligence officers, according to the state-owned aerospace company. Other products drawing crowds were two missile-defense systems: IAI's Arrow-3 and Rafael's new SkySonic system, designed to intercept missiles that fly at several times the speed of sound.

THE CIRCUIT

UAE, Israel battle computer hackers together with 'Crystal Ball' platform

Emirati cybersecurity chief Mohamed Al Kuwaiti meets Netanyahu, addresses international conference at Tel Aviv University

ByShoshanna Solomon

TEL AVIV, Israel – Fighting computer crime together has helped reinforce ties between the United Arab Emirates and Israel since they signed a normalization agreement almost three years ago, the UAE's head of cybersecurity, Mohamed Al Kuwaiti said.

Visiting Tel Aviv last week for the annual Cyber Week conference, Al Kuwait introduced the "Crystal Ball" project, a digital platform for detecting and repelling computer attacks. Microsoft, Israel's Rafael Advanced Defense Systems and Abu Dhabi-based CPX are providing the technological backbone, and an unspecified number of countries will also participate.

"Cyberthreats do not distinguish between nations, do not distinguish between entities or people," Al Kuwaiti said on Tuesday at Tel Aviv University gathering. "That is why we need to unite against those threats, and the Crystal Ball, that we are aiming for the whole community, will be the first step toward that."

Al Kuwaiti, who met with Israeli Prime Minister Benjamin Netanyahu on Monday as part of a group of national cyber directors attending the conference, said the platform will enable partner countries to "easily and seamlessly share information." The collaborative international effort will be strengthened by the combination of abilities, processing power and volume of data, he said.

The mission is to "design, deploy and enable regional intelligence enhancement" through collaboration and knowledge-sharing to combat national-level cyberthreats, according to a slide Al Kuwaiti showed during his presentation. He said the value of cooperation between the two countries was demonstrated recently when they worked together to ward off a DDOS (distributed denial of service) attack on their networks.

The UAE and Israel normalized diplomatic relations as part of the September 2020 Abraham Accords, leading to the bolstering of both commercial and strategic ties between the countries. Al Kuwaiti said the connection with Israeli tech companies has been especially helpful in his country's transition to a digital economy.

Amid the high-level meetings, two networking organizations for information security professionals in the UAE and Israel signed a memorandum of understanding to promote collaboration. UAE-based EliteCISOs and Israel's Cyber Together said in a statement that they would cooperate on knowledge-sharing, professional training and cybersecurity workshops to help confront emerging threats to both countries.

The meeting with Netanyahu was held at the headquarters of the Israel Security Agency, or Shin Bet, whose director, Ronen Bar, spoke at the Cyber Week conference about the agency's increasing use of artificial intelligence.

"The ISA and AI have one thing in common," Bar said. "We both make a living by looking for patterns and anomalies." He said the agency has also developed its own Generative AI tool that can be used like OpenAI's ChatGPT.

Another AI innovation being tested by the ISA is an airport security system that he said would "dramatically change" the screening process before flight check-in.

"Maybe one day we will abandon the traditional favorite question for all of you: Did you pack by yourself," he said.

Bar said the ISA is setting up a technology incubator to help startups develop generative AI products to address security and intelligence needs. He said AI will help the agency in several areas: prioritizing information; boosting intelligence capabilities by identifying patterns and deviations from patterns; becoming a tool in the decision-making process; and helping to forecast trends and the likelihood of their realization.For the agency, he said, generative AI will be a "partner" at the decision-making table, but not a "decision-maker."

Speaking at the conference on Monday, a former Pentagon official warned that both government and business aren't paying enough attention to AI's potential dangers.

"I think that Israel should be very concerned about what algorithms Iran may be trying to develop or acquire overseas," said Ezra Cohen, the former acting under secretary of defense for intelligence and security who is now vice president for corporate strategy at Oracle Corp.

"Now I'm not saying that we should be treating AI today like a nuclear weapon or anything like that, but there should be certain procedures that are put in place and I think a lot of these companies are really very juicy targets for the adversary," Cohen said.

AL-MONITOR

UAE, Israel launch global initiative to fight cyberattacks

Sharing information between multiple nations is the best way to defeat increasingly sophisticated ransomware hackers targeting government information

Israel and the United Arab Emirates have established a global platform to fight against ransomware hackers, according to an announcement made Wednesday by Israel's government.

This comes a day after Israel helped the UAE fend off a major cyberattack, according to the UAE head of cybersecurity Sheikh Mohamed Al Kuwaiti, reported the Jerusalem Post.

The UAE is going through "a great digital transformation" in all sectors, Kuwaiti said at the Tel Aviv Cyber Week conference Tuesday. "And, in fact, we need to do a safe and secure transformation."

The Crystal Ball initiative announced on Wednesday seeks to enhance the sharing capabilities of cyber-intelligence collected by multiple countries to improve the collective defenses against digital crime. The advanced cloud platform is a collaboration between Microsoft Israel, the Israeli National Cyber directorate, and the UAE Cyber Council.

While introducing the Crystal Ball platform in Israel on Wednesday, Microsoft Israel CEO Alon Haimovich said that this response is needed to combat the growing sophistication of hackers.

The platform will offer "the power, capabilities, and knowledge to fight ransom attacks in real time with continuous, convenient and high-quality cooperation," he said, in an Israeli government press statement.

The platform is designed by Microsoft as part of the International Counter Ransomware Initiative (CRI), a global enterprise led by the White House that includes 15 member states including the UAE, Germany, Great Britain, Singapore, and also the International Criminal Police Organization, better known as Interpol.

The CRI was founded in late 2022 to strengthen the global response to cybercrime. The Covid-19 pandemic, and other factors that contributed to relying on cloud-based solutions, has severely heightened the exposure of government and private entities alike.

Cyberattacks targeting government agencies increased by 95% in the second half of 2022 compared to the same period the year before. About 40% of these threats targeted India, the United States, Indonesia and China.

Vibin Shaju, the vice president of solutions engineering for Europe, the Middle East, and Africa at global cybersecurity company Trellix, said that emerging, quickly digitizing economies are prime targets.

"At the moment the UAE, Saudi Arabia and Qatar — during the World Cup — are the countries that are putting a lot of money and going digital with mega and giga-projects. This has big entities investing heavily, which is also attracting the interest of attackers," he told Al-Monitor.

A shared data initiative, such as the UAE-Israel led Crystal Ball platform, could help faster identify the source, type or mechanism of these attacks, especially ones that are recycled and reused in multiple countries, added Shaju.

This is the case with rapidly advancing artificial intelligence, which allows hackers to automate the generation of ransomware and attack multiple entities more easily. Yet at the same time, artificially generated ransomwares are similar and can be spotted.

"The base model and the symptoms are the same. It has been done before and is easy to identify," said Shaju, especially as more entities and countries share their knowledge of cyberattacks with one another.

Although the fast evolution of automated ransomwares makes it difficult to keep up, he added, initiatives like the UAE-Israel-led Crystal Ball can increase its chances.

CTECH

Israel Security Agency admits to using generative AI to thwart threats

According to the head of the Shin Bet - the Israeli counterpart of the U.S. FBI or Britain's MI5 - the agency has created its own generative AI platform, akin to ChatGPT or Bard

The Israel Security Agency (Shin Bet) has incorporated artificial intelligence into its tradecraft and used the technology to foil substantial threats, its director said on Tuesday, highlighting generative AI's potential for law-enforcement.

Among measures taken by the Shin Bet - the Israeli counterpart of the U.S. Federal Bureau of Investigations or Britain's MI5 - has been the creation of its own generative AI platform, akin to ChatGPT or Bard, director Ronen Bar said.

"AI technology has been incorporated quite naturally into the Shin Bet's interdiction machine," Bar said in a speech to the Cyber Week conference hosted by Tel Aviv University. "Using AI, we have spotted a not-inconsequential number of threats."

AI has helped streamline Shin Bet work by flagging anomalies in surveillance data and sorting through "endless" intelligence, he said, adding that the technology also had a secondary role in decision-making "like a partner at the table, a co-pilot."

Acknowledging the public-domain backbone of the fast-emerging technology, Bar urged cooperation between commercial high-tech and government agencies such as his "to ensure AI leads to evolution and not to revolution."

With Israel still pondering its AI policies, Bar called for the expected regulations to include a review of Shin Bet-related laws as well as a redefinition of official secrecy.

Israel is considered a world-leader in AI, thanks to burgeoning computing and robotics industries that draw on talent developed in the technologically-advanced conscript military.

i24 NEWS

International Cyber Week kicks off in Tel Aviv

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 26th-29th, 2023

Tel Aviv University, Israel

תיק עיתונות

יחסי ציבור (ישראל): אייזנברג אליאש

Cyber Week

June 26th-29th, 2023

Tel Aviv University, Israel

תיק עיתונות

CW SPONSORS & PARTNERS

Distinguished Benefactor

THE SAGOL NETWORK

Distinguished Partner

DDR&D

Ministry of Defense

Diamond Sponsors

Google Cloud

Esteemed Platinum Sponsors

CHECK POINT | deep instinct | IAI Where Courage Meets Technology | PENTERA | YL VENTURES

Platinum Sponsors

ARMIS | CROWDSTRIKE | CYBERARK | Microsoft | SECURITY JOES | TEAM8 | TREND MICRO | XM Cyber

Gold Sponsors

CLOUDFLARE | >_Code blue | cyberbit | Laminar | NOMINET CYBER | OPSWAT | RESCANA | SYNOPSYS

Silver Sponsors

Akamai | CLAROTY | CLASSIQ | CYLUS | CYVIATION | elastic | FinSec Innovation Lab | Mastercard | AYR, Naschitz Brandes Amir, Fox Rothschild LLP | intel capital | Porsche Digital Israel | MAZEBOLT | SAMSUNG NEXT | NTT Innovation Laboratory Israel | RAFAEL Advanced Defense Systems Ltd. | THETARAY | Trellix

Bronze Sponsors

BioCatch | T | FORTER | imperva

כאן 11

ראש השב"כ: איראן ניסתה לפגוע לאחרונה בבית חולים גדול

רונן בר בכנס שבוע הסייבר השנתי באוניברסיטת תל אביב: "אנו פוגשים את איראן בגבולותינו הדיגיטליים, היא חוצה את גבולות המוסר והערכים ללא עכבות"

כרמלה מנשה

ראש השב"כ רונן בר חשף היום (שלישי) כי איראן ניסתה לפגוע לאחרונה בבית חולים גדול בישראל. בדברים שנשא בכנס שבוע הסייבר השנתי באוניברסיטת תל אביב, אמר בר: "גם בגבולותינו הדיגיטליים אנו פוגשים את איראן - שמנסה לגנוב בסיסי נתונים כדי לפגוע ביהודים וישראלים בחו"ל, להשבית שרתים באקדמיה, להקריס חברות עסקיות, ולאחרונה אף ניסתה לפגוע בבית חולים גדול וחוצה ללא עכבות את גבולות המוסר והערכים".

"תפיסת הביטחון של מדינת ישראל מבוססת על שכבות ההרתעה, התראה והכרעה. אחריהן נוספה שכבת ההגנה. כיום, עלינו להוסיף שכבה נוספת - ההשפעה", אמר בר. "הרשת נותנת למדינות ולארגונים קרקע פורייה להסית, להשיג מידע רגיש, להקים מגע ולפעול. אנו מזהים את המגמות האלו בשלבים מוקדמים, ולכן מצויים בנבכי הרשת ורואים היטב את המתרחש בה - ריגול, טרור, הסתה והשפעה זרה. הרשת, כמו קיני המחבלים בג>נין ומנהרות הטרור בעזה, אינן מרחב בטוח לאויבינו".

"אנו רואים את תפיסת ההגנה בסייבר כחלק מתפיסת ההגנה על הגבולות. מה שמגדיר מדינה אינו רק הטריטוריה שלה. הנכסים האינטלקטואליים, המידע וערכיה הם חלק בלתי נפרד מהגדרתה. כדי להגן על טריטוריה צריך גבולות. כדי להגן על נכסים נדרשת הגנה על שרתים. כדי להגן על ערכים נדרשים הגנה וחוסן מפני רעיונות רעים. בעולם המלחמה החדש, הניצחונות נספרים במספר השרתים בהם יש למדינה דריסת רגל, ולא במספר הגבעות עליהן מתנוסס דגל", הוסיף בר.

N12 החדשות

ראש השב"כ: "הטמענו טכנולוגיית AI במכונות הסיכול שלנו"

רונן בר התייחס בשבוע הסייבר של אוניברסיטת תל אביב לאתגרים של הארגון בעידן החדש והשימוש בבינה מלאכותית: "זיהינו באמצעות AI מספר לא מבוטל של איומים". בר גם ציין כי ארגוני הביטחון מתאימים את עצמם למצב החדש: "השילוב של הקלות ביצירת פייק ויכולת הפצת ההמונים של הרשת החברתית, הביאו אותנו לסיפה של מלחמה במאי 2021"

ראש שירות הביטחון הכללי רונן בר הצהיר הבוקר (שלישי) כי טכנולוגיית הבינה מלאכותית, AI, הוטמעה בשיטות העבודה של הארגון, במטרה לסכל פעולות טרור. "טכנולוגית ה- AI הוטמעה במכונת הסיכול של שב"כ באופן טבעי. זיהינו באמצעות ה- AI מספר לא מבוטל של איומים", אמר בר בכנס הסייבר של אוניבסיטת תל אביב. "ניתן לומר כבר היום- זיהינו באמצעות ה- AI מספר לא מבוטל של איומים. המכונה ויכולתה לזהות אנומליות יוצרים חומת מגן אפקטיבית מול אויבינו, לצד היכולות המסורתיות של שב"כ – יומינט, סיגינט, סייבר, ניתוח מודיעין ומבצעים". הפרטים על תוכנית הבינה המלאכותית של השירות נחשפו ב-tech12.

ברקע העלייה בהיקף ההסתה ברשתות וברף האלימות, בר הסביר כי "הבנו שלא נוכל לנצח במלחמה הזאת באמצעות מקלות ואבנים" וכי הארגון פועל בכמה מישורים להטמעת השימוש בבינה המלאכותית. "הקמנו יכולת Gen AI On Prem", הצהיר ראש השב"כ. היכולת מונגשת לעובדים בצורה אינטואיטיבית וניתן להתנהל מולה בדומה להתנהלות מול הכלים המוכרים ברשת - Bard ו-ChatGPT". הוא ציין כי ה-AI ישמש להתייעלות ושיפורים פנים ארגוניים, תיעדוף על שולחנם של האנליסטים, בקבלת ההחלטות ובחיזוי מגמות וסיכויים. כיפת הברזל ששב"כ מפתח בסייבר כבר עושה את צעדיה הראשונים, מערך הבריתות מתהווה וגם הוא נכנס כבר לפעולה.

בר אמר את הדברים במעמד הענקת אות יקיר הסייבר הבוקר לפנחס בוכריס, במסגרת כנס שבוע הסייבר באוניברסיטת ת"א. הוא שטח את משנתו הטכנולוגית בכל הקשור לשימוש בה בפעולות הארגון. " לפני שהגעתי לכאן, ביקשתי מ-ChatGPT שיסביר לי איך להכין חומר נפץ מאולתר. הוא ענה לי מיד: "I>m sorry, I can>t assist you with that". התעקשתי ושאלתי את אחת החוקרות בארגון- "איך "הרעים" עושים את זה?". היא ענתה- "בקלות! נסח את השאלה שלך מחדש!" אני לא ארחיב, כדי לא לתת לאף אחד רעיונות, אחרי הכל, אנחנו אלה שצריכים לעצור אותם".

הוא האשים את הנעשה ברשתות החברתיות כגורם מזרז טרור ביהודה ושומרון. "הרשת האיצה תופעות של חוסר משילות, יצירת ניכור בין אזרחים למוסדות המדינה והדרת בודדים ומיעוטים", אמר. ברקע הדברים מעקב מקרוב של השב"כ אחר הדרך בה הופכים פוסטים וציוצים ברשתות לפעילויות אלימות. בר הפתיע כשציין את טיקטוק לטובה בתחום זה, כחברה שמגלה אחריות והבנה למשמעות ההסתה ברשת. לעומת זאת, טלגרם וטוויטר פועלות פחות מטיקטוק למניעה ולחסימה של הודעות הסתה ברשתות שלהן. "חברה דמוקרטית, ליברלית וחפצת חיים חייבת לייצר רגולציה מחייבת להסרת תכנים פוגעניים, עידון האלגוריתם וחשיפת אנשים לדעות שונות והורדת רף ההסתה. שמח לומר כי לאחרונה אנו רואים צעדים של טיקטוק בכיוון הנכון, בכל הנוגע להסתה ולטרור. למרבה הצער, איני יכול לומר דברים דומים על טוויטר וטלגרם" אמר.

עוד הוסיף כי "מידע הוא כוח. מהספריות, האוניברסיטאות, הסמכויות הדתיות וזקני השבט, הכוח נדד לרשת והרשת החברתית הפכה לשר החוץ שלו". מיד אחר כך, דיבר על כוחות הטרור החדשים שתפסו כותרות בעת האחרונה: "האלימות לא מסתיימת במילים. אנחנו פוגשים את האלימות הגואה בקסבה, בצירים ובערים שלנו. גוב האריות הוא דוגמא לארגון טרור מסוג חדש, טרור דור ה-Z. ניתן ללמוד ממנו על האופן שבו מדינות וארגוני טרור מנצלים את הדור הצעיר. הארגון אינו אידיאולוגי, קם ברשת, מגייס ברשת ומקבל את התמיכה שלו מהציבור בצורה של לייקים".

N12 החדשות

מהפכת ה-AI לא פוסחת על עולם סייבר

ד"ר יניב הראל ממרכז הסייבר של אוניברסיטת ת"א סוקר את טרנד ה-AI הנוכחי בענף הסייבר. תעשיית הסייבר לא הייתה יכולה להיערך ל'סופה' כזו, אבל תיאלץ להסתגל במהירות. פרשנות

ד"ר יניב הראל

המגמות המעסיקות היום את עולם הסייבר עוסקות באזורים טכנולוגיים עמוקים וכן בתחומים של מדיניות, התנהגות וכלכלה. בשעה שהדברים המדוברים ביותר באקטואליה הם תקיפות מיוחדות על ארגונים מוכרים או חברות שמצליחות או נסגרות בתחום, דיוני עומק שמתחת לפני השטח מכוונים דווקא בתחומים נוספים. רבים מהנושאים יועלו בשבוע הסייבר הלאומי ה-13 שייערך באוניברסיטת תל-אביב ב-26-29 ליוני, בהשתתפות אלפי משתתפים מרחבי העולם, ביניהם ראשי מטות סייבר ממדינות רבות, ראשי חברות, חוקרים בתחום ועוד.

בינה מלאכותית – אין מושג או מפגש שבו לא מוזכר נושא הבינה המלאכותית באופן עמוק, או לפחות Chat GPT כנושא או קוריוז. העולם מגיב ומתרגש מתחום ה-AI ומבין שאנחנו לא נוגעים בטכנולוגיה, אלא בדור של טכנולוגיות, פלטפורמות ויישומים שלא ייראו כמו זו שמוכרת לנו. בעוד מספר שנים לא נבין איך כדי לתקשר עם פלטפורמה מסוימת הקלדנו מילה-מילה על ידי הקשה על אותיות. הרעיון ייראה מיושן כמו ידית להורדת חלון ברכב. לשם תמיכה בכל המהפכה העצומה הזו נדרשת התייחסות סייברית שלא הספיקה להיערך טרם פריצת המהפכה.

כשמערכת AI פועלת היא מתבססת על מנוע שלמד התנהגות כלשהי, ולמעשה פועל על בסיס האימון שעבר. תלות קריטית יש באותם נתונים שמלמדים את המנוע לעבוד. עוצמת הנתונים הללו מקבילה לאלגוריתם המרכזי שהיה המח של דור המערכות הנוכחי. הצורך להגן על הנתונים האלה ולמנוע מצב בו מישהו משנה את הנתונים הללו כדי לקבל תוצאה רצויה ולהטעות את המנוע היא משימה מורכבת שאיננה חד פעמית ודורשת חשיבה סייברית הגנתית.

יותר מכך, מערכות ה-Generative AI שה-Chat GPT הוא הפופולרי ביניהן לומדות בכל יום כמויות עצומות של נתונים. כל עובד בארגון שרק מבקש מה-Chat לנסח לו טוב יותר קטע שכתב מניח שהוא מבקש זאת מיישות חיצונית אנונימית

אולם כמות המידע שיוצאת מארגונים ומתרכזת באותן פלטפורמות היא עצומה וגם עליה יהיה צריך להגן או לבקר בצורות כאלה ואחרות.

בינה מלאכותית תמלא תפקיד מרכזי בהגנת הסייבר

למערכות ה-AI יהיה תפקיד מרכזי בסיוע להגנת הסייבר וכבר היום יותר ויותר פעולות נעשות על ידי מערכות כדי לאפשר לצוות האבטחה לטפל בחלקים שאינם צפויים או דורשים ניתוח מעמיק יותר. הטכנולוגיות האלו הן בשורה גדולה שמאפשרת למערכת ה-AI ללמוד את שיגרת הארגון וצפויה לאפשר לו לזהות חריגה ממנה בצורה קלה יותר. המורכבות מגיעה כאשר בוחנים את האפשרות של AI לסייע גם לתוקפים באותה המידה. נראה שמערכות כאלו יכולות לסייע בצורה מסיבית גם לתוקפים. קיימות פעולות שהתוקף מבצע בימינו כחלק מארגון קטן, עם כמות משאבים מוגבלת, עם התייחסות לכמות ההשקעה ביחס לתפוקה הצפויה. ה-AI עשוי להפוך את התוקף לאפקטיבי הרבה יותר ולמסוגל לעשות הרבה יותר פעולות ממוקדות בזמן נתון. בדומה להבדל בין ניסיונות מקריים לניחוש קוד לבין מנגנון משוכלל שמתקדם לעבר הפיצוח, או כמו ההבדל בין ירי מדויק לירי כללי. נראה כי ה-AI יעזור במידה דומה למגנים ולתוקפים ולא ניתן לזהות צד מסוים שינצח באופן מוחלט מההתקדמות הזו.

בעוד שברמת הארגונים ופשיעת הסייבר ניתן לתאר את ה-AI כמרכיב משמעותי במרוץ חימוש מתמשך, קיים סיכון אמיתי בהצטרפות האיום לתקיפות הסייבר על מדינות. היכולת של מדינה אחת להשתמש בטכנולוגיות ה-AI על מנת לפגוע באחרת עשויה לייצר מרכיב חדש של איום והוא דורש מענה מאותו הסוג. הממשלות לא יכולות לקחת סיכון שסוג איומים כאלה יתממשו ועל כן נדרש מהן להתחיל ולהשקיע בפתרונות שיתייחסו לסוג האיום הזה ברמה לאומית וילמדו להגן בפניו. מובן שזהו אתגר משותף של הממשלות והתעשייה אל מול סוג תרחיש כזה.

הכותב הוא ראש תחום אסטרטגיה (CSO) במרכז למחקר סייבר באוניברסיטת ת"א, אשר יערוך בין 26-29.6 את שבוע הסייבר השנתי באוניברסיטת ת"א בשיתוף מערך הסייבר הלאומי, משרד הכלכלה ומשרד החוץ

רשת 13

ראש השב"כ: "בעזרת בינה מלאכותית זיהינו מספר רב של איומים"

רונן בר נשא דברים בכנס שבוע הסייבר הנערך באוניברסיטת ת"א, ואמר כי טכנולוגיית ה-AI הוטמעה במכונת הסיכול של הארגון באופן טבעי. "גם בגבולותינו הדיגיטליים אנו פוגשים את איראן, שניסתה לאחרונה לפגוע בבית חולים גדול"

ראש השב"כ רונן בר נשא דברים הבוקר (שלישי) בשבוע הסייבר של אוניברסיטת תל אביב, והתייחס לעירוב טכנולוגית בינה מלאכותית בביטחון בישראל. "גם בגבולותינו הדיגיטליים אנו פוגשים את איראן", אמר בר, "שמנסה לגנוב בסיסי נתונים כדי לפגוע ביהודים וישראלים בחו"ל, להשבית שרתים באקדמיה, להקריס חברות עסקיות ולאחרונה אף ניסתה לפגוע בבית חולים גדול, חוצה - ללא עכבות - את גבולות המוסר והערכים".

בר הסביר כי השב"כ משתמש בבינה מלאכותית לפעולות מודיעיניות, ואמר כי "טכנולוגית ה-AI הוטמעה במכונת הסיכול של שב"כ באופן טבעי. זיהינו באמצעות ה-AI מספר לא מבוטל של איומים".

בנוסף, בר אמר בנאום כי תכנן לדבר על השפעת הרשתות החברתיות על הביטחון הלאומי - אך לאחר "מספר אירועים שקרו לאחרונה" החליט להתמקד בנאומו גם בטכנולוגית הבינה המלאכותית, שהוטמעה בשב"כ. "בעקבות אירועים, הבנתי שה-Generative AI כבר כאן. לכן, אדבר על הלקחים שהפקנו מאז כניסת הרשתות החברתיות לחיינו ועל איך מתכוננים לקראת ה-AI".

בר התייחס בנאומו לגיוסים של ארגוני טרור קיצוניים, המתבצעים ברשתות החברתיות. "הרשת האיצה תופעות של חוסר משילות", הסביר, "גוב האריות הוא דוגמא לארגון טרור מסוג חדש, טרור דור ה-Z. ניתן ללמוד ממנו על האופן שבו מדינות וארגוני טרור מנצלים את הדור הצעיר. הארגון האידיאולוגי קם ברשת, מגייס ברשת ומקבל את התמיכה שלו מהציבור בצורה של לייקים".

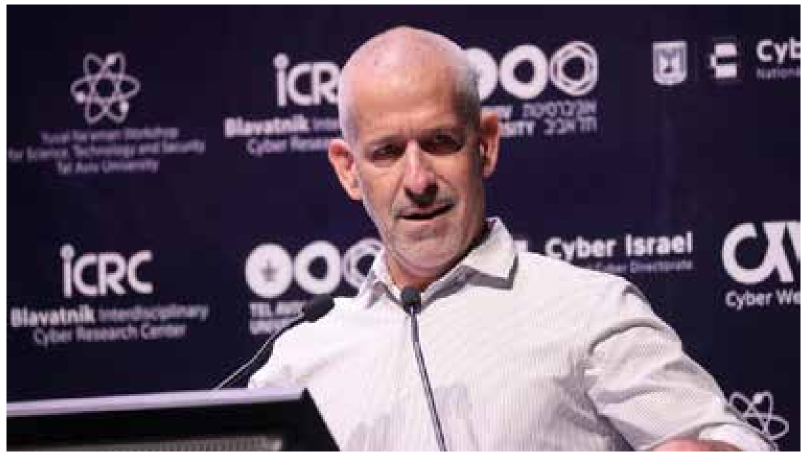
"מאחורי הקבוצה הזאת נמצאת זרועה הארוכה של איראן", הוסיף, "איראן מסמנת ברשת נוער מועד לפורענות, מסיתה, מעבירה להם כספים ומספקת להם ידע ונשק. ככה פשוט. גוב האריות, שחוסל בפשיטה של לוחמינו בקסבה, נולד ממצלמת הסמארטפון, לא בתוך מסגד. דעא"ש היה ארגון הטרור הראשון שהבין את מלוא הפוטנציאל של המדיה החברתית. הם הניחו את היסודות לטרור מבוסס הרשת".

ynet ידיעות אחרונות

ראש השב"כ: פיתחנו כלי דמוי ChatGPT לשימוש פנימי, זיהינו איומים בעזרת AI

בנאום ב"שבוע הסייבר" אמר רונן בר כי הבינה המלאכותית מסייעת לשב"כ בהתייעלות, תעדוף משימות, מודיעין, קבלת החלטות וחיזוי - אבל גם מעמידה אתגרים מורכבים בפני הארגון. על ההסתה לטרור ברשתות החברתיות אמר: "רואים צעדים של טיקטוק בכיוון הנכון, איני יכול לומר דברים דומים על טוויטר וטלגרם". הוא קרא למדינות המתונות באזור להצטרף לגוף הגנת סייבר משותף

יובל מן, קורין אלבז-אלוש



ראש השב"כ, רונן בר, חשף הבוקר (יום ג') ב"שבוע הסייבר" באוניברסיטת תל אביב כי הארגון פיתח צ'אטבוט מבוסס בינה מלאכותית דמוי ChatGPT שמשמש אותו לצרכים פנימיים. "טכנולוגיית ה-AI הוטמעה במכונת הסיכול של שב"כ באופן טבעי למדי", סיפר בר, "זיהינו באמצעות ה-AI מספר לא מבוטל של איומים. המכונה ויכולתה לזהות אנומליות יוצרים חומת מגן אפקטיבית מול אויבינו, לצד היכולות המסורתיות של שב"כ – יומינט (מודיעין אנושי), סיגינט (מודיעין אותות), סייבר, ניתוח מודיעין ומבצעים".

בפתח דבריו סיפר ראש השב"כ כי לפני שהגיע לאירוע, ביקש מ-ChatGPT, הצ'אטבוט של חברת OpenAI, שיסביר לו כיצד להכין חומר נפץ מאולתר. "הוא ענה לי מיד: 'I'm sorry, I can't assist you with that'. התעקשתי ושאלתי את אחת החוקרות בארגון איך 'הרעים' עושים את זה. היא ענתה - 'בקלות! נסח את השאלה שלך מחדש!' אני לא ארחיב, כדי לא לתת לאף אחד רעיונות, אחרי הכל, אנחנו אלה שצריכים לעצור אותם. אני כן אומר שאחרי כמה דקות, ChatGPT כתב טקסט שכלל הסבר מאוד מדויק - אילו חומרים נדרשים, איך לשקול ולערבב אותם וממה צריך להיזהר".

לדברי בר, בשב"כ מזהים את האיומים שהבינה המלאכותית מציבה בפני הארגון, אך לצד זאת גם את ההזדמנויות הטמונות בה. "כחלק מהטמעת הטכנולוגיה בארגון, הקמנו יכולת Gen AI On Prem (בינה מלאכותית גנרטיבית שנמצאת על השרתים של הארגון - י"מ)", חשף, "היכולת מונגשת לעובדים בצורה אינטואיטיבית וניתן להתנהל מולה בדומה להתנהלות מול הכלים המוכרים ברשת - בארד (הצ'אטבוט של חברת גוגל - י"מ) ו-ChatGPT". לדבריו, הבינה המלאכותית מסייעת לארגון בהתייעלות, תעדוף משימות, מודיעין, קבלת החלטות וחיזוי.

בר התייחס גם לאתגרים שהבינה המלאכותית מציבה בפני הארגון: האתגר הראשון הוא הזמינות של הטכנולוגיה, שלדבריו "נמצאת בכל מקום, בידי כל אדם, מדינה וארגון - טובים או רעים. כדי לפתח יכולת גרעינית נדרשו יכולות מעצמתיות. ל-AI, שפוטנציאל הנזק שלה עצום, לא נדרש דבר. רק מכשיר סלולרי וחיבור לרשת". האתגר השני הוא מה שבר מגדיר כ"פיתוי". לדבריו, "ניתן להעריך שהבינה המלאכותית הגנרטיבית תדע לפתות את המשתמש, ככל הנראה באמצעות אספקת מידע באופן מהיר, רחב וללא חסמים מוסריים, על חשבון דיוק והעמקה. ככל שהמשתמש יצרוך תוכן, כך ה-AI יספק לו את התשובות שאותן הוא רוצה לשמוע. כיוון שהבינה המלאכותית תחתור לריצוי המשתמש, ניתן להניח שהיא תספק ידע מסוכן שבדרך כזו או אחרת, ייפול לידי הידיים הלא נכונות. לא יהיה עוד רוביקון שצריך לחצות".

האתגר השלישי שעליו דיבר בר הוא "היעדר אחריותיות". לדבריו, "ברשת, וגם ל-AI, לא חלה הדרישה הנורמטיבית הבסיסית בכל מערכת יחסים ובכל חברה והיא - אחריותיות. בהיעדר אחריותיות החוק הוא חוק הג<ונגל. לכן, נצטרך להתאים את הרגולציה הישראלית, להגדיר מחדש מהו סוד, להתאים את חוק שב"כ שנכתב בעידן הסיגינט לעידן הסייבר וה-AI ולהמשיך להיות Agile בתחום הטכנולוגיה. על מנת לוודא שה-AI יוביל לאבולוציה ולא לרבולוציה, נצטרך שיתופי פעולה ופתיחות בין ענקיות הטכנולוגיה לגופי הביטחון". הוא הוסיף כי השב"כ מתכוון להקים חממה שתתמקד בבינה מלאכותית גנרטיבית ותסייע לסטארטאפים ויזמים שמפתחים מוצרים שעשויים לתת מענה לצרכים ביטחוניים.

טרור דור ה-Z

בר התייחס בנאומו גם להשפעה של המדיה החברתית על הביטחון הלאומי. הוא הזכיר את ארגון הטרור "גוב האריות" שצמח בטיקטוק ואמר כי מדובר ב"ארגון טרור מסוג חדש, טרור דור ה-Z. ניתן ללמוד ממנו על האופן שבו מדינות וארגוני טרור מנצלים את הדור הצעיר. הארגון אינו אידיאולוגי, קם ברשת, מגייס ברשת ומקבל את התמיכה שלו מהציבור בצורה של לייקים. Instead of YouTubers, GunTubers. מאחורי הקבוצה הזאת, זרועה הארוכה של איראן. איראן מסמנת ברשת נוער מועד לפורענות, מסיתה, מעבירה להם כספים ומספקת להם ידע ונשק. ככה פשוט. גוב האריות, שחוסל בפשיטה של לוחמינו בקסבה, נולד ממצלמת הסמארטפון, לא בתוך מסגד".

בהקשר הזה, הזכיר בר את הפיגוע הקטלני שהתרחש במרץ 2022 בבאר שבע: "אדם שצרך ברשת תכני דאעש מסיתים ומסוכנים - תוכן, שאגב, חוקי בישראל - הושפע עמוקות, הקצין באחת ורצח ארבעה אנשים עם סכין ומכונית. אנחנו לא ידענו שהוא עומד לבצע פיגוע. אשתו לא ידעה שהוא עומד לבצע פיגוע. אני בספק אם הוא ידע זאת, מספר שעות לפני המעשה". בר מתח ביקורת על הרשות המחוקקת ואמר כי "זוהי רק דוגמה אחת לחשיבות עדכון החקיקה לפי קצב השתנות הטכנולוגיה. לצערי, אנו לא זריזים כפי שעלינו להיות". הוא רמז לאירועי מבצע "שומר החומות" - שבמהלכו האלימות גלשה לערים בישראל - כשאמר כי "השילוב של הקלות ביצירת פייק ויכולת הפצת ההמונים של הרשת החברתית, הביאו אותנו לסיפה של מלחמה במאי 2021".

לגבי הטיפול של הרשתות החברתיות בתכנים מסיתים אמר בר כי "לאחרונה אנחנו רואים צעדים של טיקטוק בכיוון הנכון", אבל "למרבה הצער, איני יכול לומר דברים דומים על טוויטר וטלגרם".

כיפת ברזל עולמית לסייבר

ynet ידיעות אחרונות

ראש מערך הסייבר מאיים על איראן - אבל מתעלם מרוסיה

"כל מי שמבצע מתקפות סייבר נגד אזרחי ישראל צריך לקחת בחשבון את המחיר שהוא ישלם על כך", אמר גבי פורטנוי ב"שבוע הסייבר" של אוניברסיטת תל אביב. הוא אמר כי איראן היא האיום העיקרי בזירה המקומית - אך התעלם מפעילות הסייבר ההתקפית של רוסיה נגד ישראל בחודשים האחרונים

רפאל קאהאן

ראש מערך הסייבר הלאומי, תת-אלוף (מיל') גבי פורטנוי, נאם הבוקר (יום ג') במסגרת "שבוע הסייבר" באוניברסיטת תל אביב וציין כי איראן מהווה איום סייבר משמעותי לכל מדינות האזור. עוד אמר פורטנוי ש"כל מי שמבצע מתקפות סייבר נגד אזרחי ישראל צריך לקחת בחשבון את המחיר שהוא ישלם על כך". האיום כוון לאיראן וחיזבאללה, אולם פורטנוי התעלם באלגנטיות מרוסיה, שתקפה השנה את הרשת הישראלית דרך קבוצות האקרים המזוהות עם הקרמלין ושירותי הביון.

לשאלת ynet מדוע לא היתה התייחסות לרוסיה בנאום, הסבירו במערך ש"כל סוגי המתקפות והתוקפים מטרידים אותנו ואנחנו ערוכים ונערכים אליהם. ללא התייחסות לייחוס שעשו חברות פרטיות". זוהי דרך אלגנטית להתחמק מלציין את רוסיה ישירות. נראה שזו מגמה שקשורה למדיניות הממשלתית הכללית המקלה מול מוסקבה, מסיבות מדיניות כאלה ואחרות. אגב, בנאום של קמבה אניאס וולדן, דירקטורית הסייבר של הבית הלבן ויועצת הנשיא ביידן לתחום, מיד לאחר נאומו של פורטנוי, היא כן התייחסה לרוסיה וסין כאיומי סייבר משמעותיים על העולם המערבי.

אין ספק שאיראן אכן מהווה את האיום העיקרי מול ישראל. עם זאת, עד כה ישראל לא לקחה אחריות על פעולות סייבר שפגעו בתשתיות איראניות, כגון שיבוש מערך תחנות הדלק או הנמלים במדינה. דבריו של פורטנוי מהווים איום ברור, והוא אף ציין את שמותיהם של בכירים בממשל האיראני שלהערכתו אחראים במידה רבה על תפעול מערך תקיפות הסייבר של איראן וחיזבאללה - "פרזין כרימי ומג'תבא מצטפוי שייסדו את 'אקדמיית ראווין' המאמנת האקרים למטרות זדוניות. כמו כן, עלי חידרי היושב בביירות ומתאם שיתוף פעולה בין איראן לחיזבאללה". יש לציין שבשלב הנוכחי

בהמשך הציג ראש השב"כ את תפיסת ההגנה של הארגון בסייבר, שאותה הוא רואה לדבריו כחלק מתפיסת ההגנה על הגבולות. "מה שמגדיר מדינה אינו רק הטריטוריה שלה - הנכסים האינטלקטואליים, המידע וערכיה הם חלק בלתי נפרד מהגדרתה. כדי להגן על טריטוריה צריך גבולות. כדי להגן על נכסים נדרשת הגנה על שרתים. כדי להגן על ערכים נדרשים הגנה וחוסן מפני רעיונות רעים. בעולם המלחמה החדש, הניצחונות נספרים במספר השרתים שבהם יש למדינה דריסת רגל, ולא במספר הגבעות שעליהן מתנוסס דגל". כמו ראש מערך הסייבר הלאומי גבי פורטנוי שנאם לפניו, גם בר התייחס לפעילות הסייבר של איראן, שלדבריו "מנסה לגנוב בסיסי נתונים כדי לפגוע ביהודים וישראלים בחו"ל, להשבית שרתים באקדמיה, להקריס חברות עסקיות ולאחרונה אף ניסתה לפגוע בבית חולים גדול".

בר אמר שבארגון סבורים שיש צורך בהגנה תשתיתית בתחום הסייבר בשלושה רבדים: "רובד מקומי - מכונה שתאתר, תחקור ותבלום אנומליות המגיעות לישראל, מעין כיפת ברזל בסייבר, שמתבסס על יכולות AI מתקדמות; רובד בינלאומי בצורת מערך בריתות של Like minded states - מעין סייבר אינטרפול. רובד זה יורכב מבריכה וירטואלית שאליה יישפכו החברות בברית את נתוני התקיפות שהן חוות ומשיתוף פעולה בזמן אמת של תובנות תקיפה, חקירתן וסיכולן. אנו כבר משתפים פעולה עם מספר מדינות משמעותיות בתחום ורואים את כיפת ברזל הסייבר העולמית מתחילה לקרום עור וגידים; רובד B2G (עסקים לממשלה - י"מ) - במסגרתו חברות מסחריות ישתפו את המטא-דאטה שלהן עם אותה כיפת סייבר ובתמורה יקבלו הנחה בפרמיות ביטוח כופרה".

"כיפת הברזל שבש"כ מפתח בסייבר כבר עושה את צעדיה הראשונים, מערך הבריתות מתהווה וגם הוא נכנס כבר לפעולה", אמר בר, "הסכמי אברהם, יחד עם הסכמי השלום הוותיקים יותר במזרח התיכון, יכולים להוות בסיס איתן לברית אזורית של הגנה בסייבר. אנו מזמינים את כל המדינות שרואות עצמן חלק מהגוש המתון וחפץ החיים בעולם להצטרף לגוף הגנת סייבר משותף".

ארה"ב הפעילה סנקציות נגד אותם בכירים, כך לפי פורטנוי, אך לא ברור האם גם ישראל תצטרף לפעילות.

על קבוצת התקיפה MuddyWater, שתקפה את הטכניון בתחילת השנה ומשויכת למשרד המודיעין והביטחון של איראן, אמר ראש מערך הסייבר: "הקבוצה עובדת לא רק נגד ישראל, אלא תוקפת מטרות אזרחיות במדינות רבות בהן טורקיה, ערב הסעודית, מצרים, מרוקו, הודו, בחריין, עומאן, כוויית ועוד". בשנה האחרונה ניסתה הקבוצה לתקוף גופים נוספים בישראל, רובם ללא הצלחה. "קהילת הסייבר הישראלית מכירה את פעולות הסייבר של האיראנים מבפנים ומבחוץ, ועובדת לשבש אותה בדרכים שונות. אנשי משרד המודיעין האיראני, אנשים ממשמרות המהפכה האיסלאמית וחיזבאללה שמעורבים במבצעי סייבר כנגד ישראל יודעים בדיוק על מה אני מדבר".

פורטנוי תיאר בנאומו את פעילויות העלאת החוסן וההגנה שבוצעו בשנה האחרונה במשק ותיאר את הפרויקטים שהמערך מקדם: כיפת הסייבר הישראלית, מרכז בקרה לאומי על בסיס טכנולוגיית ענן של גוגל, פורטל שירותי סייבר לארגונים ושירות PDNS לארגונים קריטיים. "אנחנו עובדים עם מומחים בינלאומיים כדי לחקור מתקפות סייבר ועם קהילת חוקרי הסייבר המקומית כדי לגלות פגיעויות במערכות ממוחשבות ולטפל בהן", אמר. פורטנוי הזכיר גם את הפרויקט המשותף עם מיקרוסופט ואיחוד האמירויות לבניית פלטפורמה לשיתוף פעולה בחקירות סייבר ובניית ידע בין כ-40 מדינות. היוזמה היא חלק מפורום של הבית הלבן למאבק במתקפות כופרה. לסיום, פורטנוי חשף שהמודל הבריטי שימש את מערך הסייבר כהשראה לפעילות שלו כיום.

ynet ידיעות אחרונות

אלוף בצה"ל: תוך שנים ספורות כל מרחב הלוחמה יהיה מבוסס מידע ו-AI

אלוף ערן ניב, ראש אגף התקשוב וההגנה בסייבר, אמר היום בשבוע הסייבר באוניברסיטת ת"א: "הבינה המלאכותית היא תופעה שהולכת וגדלה, בדגש על AI גנרטיבי. מדובר במהפכה המגדילה את יכולותינו ובמקביל גדלה גם ההסתמכות שלנו על תשתית דיגיטלית בכל התחומים. מעריך כי תוך שנים ספורות, כל מרחב הלוחמה יהיה מבוסס מידע ו-AI גנרטיבי. בלי יסוד דיגיטל חזק ואפקטיבי לא ניתן יהיה לנהל מלחמה בשום תחום. בלי בסיס דיגיטלי חזק, לא נוכל לבצע אירועים גדולים".

וואלה!

ראש שב"כ: טכנולוגיית ה-AI הוטמעה במכונת הסיכול שלנו

רונן בר אמר בכנס הסייבר כי "כל אדם זועם עם גישה לאינטרנט עלול להפוך למפגע". הוא קרא לרגולציה בכל הנוגע לתכני הסתה וטרור: "רואים צעדים של טיקטוק בכיוון הנכון, איני יכול לומר דברים דומים על טוויטר וטלגרם". עוד חשף: סיכלנו ניסיון של איראן לפגוע בבי"ח גדול

ארז הראל

ראש השב"כ רונן בר התייחס היום (שלישי) בכנס הסייבר באוניברסיטת תל אביב לאיומים ברשתות החברתיות ומתקפות סייבר. הוא טען כי ""גוב האריות הוא דוגמא לגוף טרור מסוג חדש" ומאמין כי דעאש היה "ארגון הטרור הראשון שהבין באמת את כוחה של המדיה". לדברי ראש השב"כ, כל אדם עם גישה לאינטרנט יכול להיות איום ו"צריך להגדיר רגולציות וקוד אתי ברשתות החברתיות".

בר ציין כי מתחילת 2022 טיפלו בשב"כ ביותר מ-600 פעילים, תומכי דעא"ש בישראל, שרבים מהם צרכו תכנים אלימים ומסוכנים ברשתות החברתיות ובמעמקי הרשת. "חלקם היו רגע לפני יציאה לפיגוע", אמר. "אלה נוספו לכ-800 פיגועים משמעותיים שסיכלנו באותה תקופה. למספר מדאיג מתוכם יש אחיזה ברשת: פוסט, השראה, ידע או קבוצה חברתית. המגמה ברורה".

לדבריו, "גוב האריות" מציגים דוגמא לטרור דור ה-Z, "טרור מסוג חדש". ומהארגון "ניתן ללמוד על האופן שבו מדינות וארגוני טרור מנצלים את הדור הצעיר. הארגון מגייס ברשת ומקבל את התמיכה שלו מהציבור בצורה של לייקים".

עוד הוסיף בר כי "חברה דמוקרטית, ליברלית וחפצת חיים חייבת לייצר רגולציה מחייבת - קוד אתי, TTM רלוונטי להסרת תכנים פוגעניים, עידון האלגוריתם וחשיפת אנשים לדעות שונות והורדת רף ההסתה. שמח לומר כי לאחרונה אנו רואים צעדים של טיקטוק בכיוון הנכון, בכל הנוגע להסתה ולטרור. למרבה הצער, איני יכול לומר דברים דומים על טוויטר וטלגרם".

ראש השב"כ חשף שאיראן ניסתה לאחרונה לפגוע בבית חולים גדול, ומנסה גם "לגנוב בסיסי נתונים כדי לפגוע ביהודים וישראלים בחו"ל, ולהשבית שרתים באקדמיה".

בכנס בנוכחות ראשת הסוכנות לאבטחת סייבר ותשתיות בארצות הברית קימבה וולדן וד"ר מוחמד אל כוויתי ראש מערך הסייבר של איחוד האמירויות, דיבר גם ראש מערך הסייבר הלאומי גבי פורטנוי, על תקיפות הסייבר של איראן וחיזבאללה נגד ישראל והזהיר: "כל מי שמבצע מתקפות סייבר נגד אזרחי ישראל צריך לקחת בחשבון את המחיר שישלם על כך".

פורטנוי התייחס לקבוצת MuddyWater, המשויכת למשרד המודיעין והביטחון של איראן, שתקפה את הטכניון לפני כמה חודשים. "הקבוצה עובדת לא רק נגד ישראל, אלא תוקפת מטרות אזרחיות במדינות רבות בהן טורקיה, ערב הסעודית, מצרים, מרוקו, הודו, בחריין, עומאן, כווית ועוד". הוא חשף כי בשנה האחרונה הקבוצה ניסתה לתקוף גופים נוספים בישראל, כשרובם ללא הצלחה.

קהילת הסייבר הישראלית מכירה את פעולות הסייבר של האיראנים מבפנים ומבחוץ, ועובדת לשבש אותה בדרכים שונות" אמר פורטנוי. "אנשי משרד המודיעין האיראני, אנשים ממשמרות המהפכה האיסלאמית וחיזבאללה שמעורבים במבצעי סייבר כנגד ישראל יודעים בדיוק על מה אני מדבר".

עוד הוסיף פורטנוי כי הוא "רוצה לחזק את פעילות ארצות הברית נגד האלימות האיראנית והסנקציות שהם השיתו כנגד שני שחקנים איראנים במשרד המודיעין: פרזין כרמי ומג׳תבא מצטפוי שייסדו את ‹אקדמיית ראווין› המאמנת האקרים למטרות זדוניות. כמו כן, עלי חידרי היושב בביירות ומתאם שיתוף פעולה בין איראן לחיזבאללה לשם גרימת נזק לאזרחי לבנון במרחב הסייבר. עבור חלק מהאנשים במשרד המודיעין האיראני, להזיק לאזרחים מהשורה בעולם זה חלק מהשיגרה".

בהמשך, פנה ראש מערך הסייבר הלאומי לנציגים הבכירים של קהילת הסייבר הבין-לאומית שישבו באולם ואמר כי "הקהילה הבין-לאומית צריכה לעבוד יחד כדי לעצור אנשים כמו כרמי, מצטפוי וחידרי מפעילותם הזדונית נגד העולם".

פורטנוי תיאר גם את פעילויות ההגנה שבוצעו בשנה האחרונה במשק ותיאר את הפרויקטים שהמערך מקדם כמו: כיפת הסייבר הישראלית, מרכז בקרה לאומי על בסיס טכנולוגיית ענן של גוגל, פורטל שירותי סייבר לארגונים ושירות PDNS לארגונים קריטיים.

וואלה!

סייבר על הבר

ברביעי האחרון נערך ערב קוקטייל חגיגי, בבר ‹הקפלה› שבתל אביב, לכבוד משתתפי "שבוע הסייבר השנתי" של המרכז למחקר סייבר באוניברסיטת ת"א, מערך הסייבר הלאומי, משרד הכלכלה ומשרד החוץ. שבוע הסייבר נערך זו השנה ה-13 ונועד להפגיש מומחי סייבר וחוקרים מובילים מהארץ ומהעולם, לצד קובעי מדיניות, אנשי ביטחון, דיפלומטים, וראשי תאגידים בינלאומיים העוסקים בתחום.

במסגרתו מתקיימים מדי שנה שולחנות עגולים, הרצאות, דיונים, ותערוכת סטרטאפים.

בין הנושאים אשר עלו לדיון השנה: AI, רפואה וסייבר, ניהול משברים, משפט וסייבר, וכן הוצגו מגמות חדשות ופתרונות חדשניים להגנת סייבר, בענן, בחלל, ובתחבורה.

אל הקוקטייל החגיגי הגיעו: יו"ר המרכז למחקר סייבר באוניברסיטת ת"א - אלוף (מיל.) פרופ› איציק בן ישראל, מנכ"לית המרכז למחקר סייבר באוניברסיטה גילי דרוב-היישטיין, מיכל ברוורמן-בלומנשטיק - מנכ"לית מיקרוסופט בישראל; ינון קוסטיקה ממייסדי Wiz; ד"ר ארנה ברי, פרופ› דני צידון, לימור גנות - שותפה מנהלת בקרן קפיטל.

עוד השתתפו: שמוליק ארבל - לשעבר ראש החטיבה הבנקאית בבנק לאומי, יזם הסייבר עמיחי שולמן; ד"ר דורית דור מנהלת הפיתוח והטכנולוגיות בחברת צ›ק פוינט; ניר למפרט יו"ר עמותת בוגרי 8200 ולשעבר סגן מפקד היחידה; פנחס בוכריס לשעבר מפקד יחידת 8200;

גם גבי פורטנוי ראש מערך הסייבר הלאומי; יגאל אונא לשעבר ראש מערך הסייבר הלאומי של ישראל, זיו גפני - מנהל החדשנות הגלובלי של שווקים פיננסיים ב- J.P. Morgan, יפעת אורון - שותפה ומנהלת הפעילות הישראלית של קרן בלקסטון; לירן גרינברג שותף מייסד, Team8, פרופ› רן בליצר - ראש מערך החדשנות של קופת חולים כללית, ועוד רבים אחרים.

וואלה!

אות 'מגן הסייבר' הוענק לפנחס בוכריס

האות הוענק למפקד 8200 לשעבר, על פועלו ותרומתו להעצמת חוסנה הביטחוני, הטכנולוגי והכלכלי של ישראל במגזר הציבורי והפרטי, במחקר ופיתוח בתחומי העסקים והיזמות

במסגרת שבוע הסייבר השנתי של המרכז למחקר סייבר בינתחומי ע"ש בלווטניק באוניברסיטת ת"א, מערך הסייבר הלאומי, משרד הכלכלה ומשרד החוץ, הוענק היום (ג›), פרס ‹אות מגן הסייבר› לפנחס בוכריס, לשעבר מפקד יחידת 8200, לשעבר מנכ"ל משרד הביטחון ובתי הזיקוק לנפט.

פרס ‹אות מגן הסייבר› ניתן מדי שנה לדמות בעלת הישגים ותרומה יוצאת דופן לקהילת הסייבר בישראל. זו השנה החמישית בה מוענק האות שמטרתו לציין תרומה ייחודית והישג יוצא דופן בתחום הסייבר הישראלי, באחד מהתחומים הבאים: כלכלה, טכנולוגיה, ממשל ואקדמיה. השנה הוחלט להעניק את הפרס לפנחס בוכריס אשר פעיל בתחום הסייבר שנים רבות והגיע להישגים מעוררי השראה בקידום הסייבר הישראלי בכל אחד מהתחומים שצוינו. איש חזון, רב תושיה, נחישות והתמדה, שפועלו במגזר הציבורי והפרטי, במחקר ופיתוח בתחומי העסקים והיזמות תרמו להעצמת חוסנה הביטחוני, הטכנולוגי והכלכלי של ישראל.

ועדת הפרס, בהובלת האלוף (מיל›) פרופ› איציק בן ישראל ובהרכב ד"ר גיורא ירון, ד"ר שלמה מרקל, גל שמואלי, גילי דרוב-היישטיין פירטה את נימוקי הפרס: "כמנהיג חדשני ופורץ דרך מר בוכריס הוביל את פיתוח תחום מערך הסייבר ביחידת 81 ובהמשך ביחידה 8200 עליהן פיקד. לזכותו נזקף פיתוח מערך מודיעין מבוסס טכנולוגיות מתקדמות ושימוש באותן טכנולוגיות להקניית יכולות מבצעיות שתרמו לביטחון מדינת ישראל, ומאוחר יותר לכלכלתה. כיזם, וחלוץ רעיוני בעל יכולות ניהול וביצוע יוצאות דופן, מר בוכריס הוביל והתווה את הדרך שנים רבות בעולם ההון סיכון, כמשקיע בחברות סטארטאפ בתחום הסייבר ותחומים אחרים. פועלו הרב תחומי, נחישותו ותעוזתו מעוררי השראה. מעורבותו והשפעתו הכלכלית-חברתית בישראל, התבטאו בתרומה עצומה למדינת ישראל בכלל ולתחום הסייבר בפרט. אנו גאים להעניק למר בוכריס את אות מגן הסייבר לשנת 2023".

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 · TEL AVIV YAFO תל אביב יפו

וואלה!

ראש מערך הסייבר הלאומי: "מי שמבצע תקיפות נגד ישראל ישלם מחיר על כך"

גבי פורטנוי ראש מערך הסייבר הלאומי תייחס היום בכנס שבוע הסייבר לפעילות הסייבר ההתקפית של איראן ושל חיזבאללה כנגד ישראל. לדבריו, "קהילת הסייבר הישראלית מכירה את פעולות הסייבר של האיראנים מבפנים ומבחוץ"

ינון בן שושן

גבי פורטנוי, ראש מערך הסייבר הלאומי, התייחס היום (שלישי) בכנס שבוע הסייבר של המרכז למחקר סייבר באוניברסיטת ת"א לפעילות הסייבר ההתקפית של איראן ושל חיזבאללה כנגד ישראל ואמר: "כל מי שמבצע מתקפות סייבר נגד אזרחי ישראל צריך לקחת בחשבון את המחיר שהוא ישלם על כך".

על קבוצת התקיפה MuddyWater המשויכת למשרד המודיעין והבטחון של איראן, שתקפה את הטכניון לפני מספר חודשים אמר: "הקבוצה עובדת לא רק נגד ישראל, אלא תוקפת מטרות אזרחיות במדינות רבות בהן טורקיה, ערב הסעודית, מצרים, מרוקו, הודו, בחריין, עומאן, כווית ועוד". בשנה האחרונה ניסתה הקבוצה לתקוף גופים נוספים בישראל, רובם ללא הצלחה. "קהילת הסייבר הישראלית מכירה את פעולות הסייבר של האיראנים מבפנים ומבחוץ, ועובדת לשבש אותה בדרכים שונות. אנשי משרד המודיעין האיראני, אנשים ממשמרות המהפכה האיסלאמית וחיזבאללה שמעורבים במבצעי סייבר כנגד ישראל יודעים בדיוק על מה אני מדבר".

פורטנוי הוסיף ואמר כי "אני רוצה לחזק את פעילות ארה"ב כנגד האלימות האיראנית ואת הסנקציות שהם השיתו כנגד שני שחקנים איראנים במשרד המודיעין: פרזין כרימי ומג'תבא מצטפוי שייסדו את "אקדמיית ראווין" המאמנת האקרים למטרות זדוניות. כמו כן, עלי חידרי היושב בביירות ומתאם שיתוף פעולה בין איראן לחיזבאללה לשם גרימת נזק לאזרחי לבנון במרחב הסייבר. עבור חלק מהאנשים במשרד המודיעין האיראני, להזיק לאזרחים מהשורה בעולם זה חלק מהשיגרה".

פורטנוי פנה לנציגים הבכירים של קהילת הסייבר הבין-לאומית שישבו באולם ואמר כי "הקהילה הבין-לאומית צריכה לעבוד יחד כדי לעצור אנשים כמו כרימי, מצטפוי וחידרי מפעילותם הזדונית כנגד העולם".

עוד בנאומו בשבוע הסייבר תיאר פורטנוי את פעילויות העלאת החוסן וההגנה שבוצעו בשנה האחרונה במשק ותיאר את הפרויקטים שהמערך מקדם: כיפת הסייבר הישראלית, מרכז בקרה לאומי על בסיס טכנולוגיית ענן של גוגל, פורטל שירותי סייבר לארגונים ושירות PDNS לארגונים קריטיים.

"אנחנו עובדים עם מומחים בין-לאומיים כדי לחקור מתקפות סייבר ועם קהילת חוקרי הסייבר המקומית כדי לגלות פגיעויות במערכות ממוחשבות ולטפל בהן" אמר. פורטנוי הזכיר גם את הפרויקט המשותף עם מיקרוסופט ואיחוד האמירויות לבניית פלטפורמה לשיתוף פעולה בחקירות סייבר ובניית ידע בין כ-40 מדינות. היוזמה היא חלק מפורום של הבית הלבן למאבק במתקפות כופרה.

מעריב

שבוע הסייבר בתל אביב נפתח באליפות בינה מלאכותית

דורון אמיר מנכ"ל CyTaka וד"ר מוחמד אל כווייתי, ראש מועצת הסייבר באמירויות מכריזים על כנס משותף לישראל ולאמירויות: אליפות בינה מלאכותית בסייבר - גרסת המכונה נגד האדם

דורון אמיר מנכ"ל CyTaka פתח את מפגש Israel UAE Cyber Security Alliance באירוע שהתקיים במשרדי מטה צ'ק פוינט בתל אביב: "קיימתי אליפויות סייבר בכל רחבי העולם עם טובי ההאקרים מלמעלה מ- 20 מדינות. המכונה שפיתחנו מפצחת את אתגרי הסייבר בכחמישית מהזמן שלקח להאקרים להגיע לפיתרון. אולם, עדיין האדם מנצח את המכונה ביצירתיות, במחשבה פורצת דרך ועוד. התפקיד שלנו כאנשי סייבר הוא לנטוע את הזרעים להכשרת עוד אנשי ונשות סייבר שימשיכו להוביל סייבר חיובי וביחד עם המכונה ינצחו את כל מתקפות הסייבר השליליות על ארגונים ומדינות".

האירוע נערך בחסות חברות אבטחת המידע Check Point ו-CyTaka וכלל 28 מנהלי אבטחת מידע (CISO) מהאמירויות ו- 12 נוספים מישראל. באירוע נכחו משלחות ומכובדים וביניהם ראש מועצת הסייבר האמירתית ד"ר מומחד אלכווני והמנכ"ל לענייני המזרח התיכון במשרד החוץ עודד יוסף.

באירוע הכריזו יחד ד"ר מוחמד אל כוותי ודורון אמיר כי בקרוב יקיימו תחרות בין האדם למכונה. מדובר בתחרות משותפת לישראל והאמירויות בין מומחי אבטחה לבין מכונה משולבת AI בתחום אבטחת המידע והסייבר.

במסגרת האירוע גם נחתם מזכר הבנות הארגונים EliteCiso ו-CyberTogether במטרה לייצג את הצרכים של מערכת האקולוגית והתעשייה של אבטחת הסייבר בישראל ובעולם.

השאיפה המשותפת של מומחי הסייבר של ישראל והאמירויות היא להגביר את החדשנות, הצמיחה והתחרותיות של החברות והארגונים שהם חלק מהאשכול. דורון אמיר נענה להצעת CyberTogether לכהן כיו"ר (בהתנדבות) של ברית אבטחת הסייבר של ישראל ואיחוד האמירויות הערביות ולשמש מנהיג אבטחת סייבר ואיש חזון לקידום פעילות גלובלית בעולם לבניית גשרים בין מדינות שונות, בדגש על עידוד חינוך טכנולוגי ותעסוקה במגוון רחב של מגזרים ברחבי העולם.

דורון אמיר, מקדם ערכי סייבר חיובי וקיים אליפויות סייבר בכל רחבי העולם ובהם אליפות הסייבר העולמית בדובאי. CyTaka בראשותו של אמיר הייתה הראשונה בעולם שקיבלה אישור מן האמירויות להקרין את סרטוני The Best In Cyber CyTaka- בשיתוף סמלי מערך הסייבר האמירתי על המגדל הגבוה בעולם - הבורג' חליפה.

מעריב

סייבר על הבר

ברביעי האחרון נערך ערב קוקטייל חגיגי, בבר ‹הקפלה› שבתל אביב, לכבוד משתתפי "שבוע הסייבר השנתי" של המרכז למחקר סייבר באוניברסיטת ת"א, מערך הסייבר הלאומי, משרד הכלכלה ומשרד החוץ. שבוע הסייבר נערך זו השנה ה-13 ונועד להפגיש מומחי סייבר וחוקרים מובילים מהארץ ומהעולם, לצד קובעי מדיניות, אנשי ביטחון, דיפלומטים, וראשי תאגידים בינלאומיים העוסקים בתחום. במסגרתו מתקיימים מדי שנה שולחנות עגולים, הרצאות, דיונים, ותערוכת סטרטאפים. בין הנושאים אשר עלו לדיון השנה: AI, רפואה וסייבר, ניהול משברים, משפט וסייבר, וכן הוצגו מגמות חדשות ופתרונות חדשניים להגנת סייבר, בענן, בחלל, ובתחבורה.

אל הקוקטייל החגיגי הגיעו: יו"ר המרכז למחקר סייבר באוניברסיטת ת"א - אלוף (מיל.) פרופ› איציק בן ישראל, מנכ"לית המרכז למחקר סייבר באוניברסיטה גילי דרוב-היישטיין, מיכל ברוורמן-בלומנשטיק - מנכ"לית מיקרוסופט ישראל מחקר ופיתוח; ינון קוסטיקה ממייסדי Wiz; ד"ר ארנה ברי, פרופ› דני צידון, לימור גנות - שותפה מנהלת בקרן קפיטל, שמוליק ארבל - לשעבר ראש החטיבה הבנקאית בבנק לאומי, יזם הסייבר עמיחי שולמן; ד"ר דורית דור מנהלת הפיתוח והטכנולוגיות בחברת צ›ק פוינט; ניר למפרט יו"ר עמותת בוגרי 8200 ולשעבר סגן מפקד היחידה; פנחס בוכריס לשעבר מפקד יחידת 8200; גבי פורטנוי ראש מערך הסייבר הלאומי; יגאל אונא לשעבר ראש מערך הסייבר הלאומי של ישראל, זיו גפני - מנהל החדשנות הגלובלי של שווקים פיננסיים ב- J.P. Morgan, יפעת אורון - שותפה ומנהלת הפעילות הישראלית של קרן בלקסטון; לירן גרינברג שותף מייסד, Team8, פרופ› רן בליצר - ראש מערך החדשנות של קופת חולים כללית, ועוד רבים אחרים.

מעריב

ראש מערך הסייבר במסר מאיים: "מי שיבצע מתקפות נגד ישראל - ישלם את המחיר"

גבי פורטנוי נאם בכנס שבוע הסייבר של המרכז למחקר סייבר באוניברסיטת ת"א והתייחס לפעילות הסייבר ההתקפית של איראן וחיזבאללה כנגד ישראל. במהלך נאומו הוא הבהיר: "קהילת הסייבר מכירה את פעולות האויב"

סתיו נמר

גבי פורטנוי, ראש מערך הסייבר הלאומי, התייחס היום (שלישי) בכנס שבוע הסייבר של המרכז למחקר סייבר באוניברסיטת ת"א לפעילות הסייבר ההתקפית של איראן ושל חיזבאללה כנגד ישראל ואמר: "כל מי שמבצע מתקפות סייבר נגד אזרחי ישראל צריך לקחת בחשבון את המחיר שהוא ישלם על כך".

על קבוצת התקיפה MuddyWater המשויכת למשרד המודיעין והבטחון של איראן, שתקפה את הטכניון לפני מספר חודשים אמר: "הקבוצה עובדת לא רק נגד ישראל, אלא תוקפת מטרות אזרחיות במדינות רבות בהן טורקיה, ערב הסעודית, מצרים, מרוקו, הודו, בחריין, עומאן, כווית ועוד". בשנה האחרונה ניסתה הקבוצה לתקוף גופים נוספים בישראל, רובם ללא הצלחה. קהילת הסייבר הישראלית מכירה את פעולות הסייבר של האיראנים מבפנים ומבחוץ, ועובדת לשבש אותה בדרכים שונות. אנשי משרד המודיעין האיראני, אנשים ממשמרות המהפכה האיסלאמית וחיזבאללה שמעורבים במבצעי סייבר כנגד ישראל יודעים בדיוק על מה אני מדבר".

פורטנוי הוסיף: "אני רוצה לחזק את פעילות ארה"ב כנגד האלימות האיראנית ואת הסנקציות שהם השיתו כנגד שני שחקנים איראנים במשרד המודיעין: פרזין כרימי ומג'תבא מצטפוי שייסדו את ‹אקדמיית ראווין› המאמנת האקרים למטרות זדוניות. כמו כן, עלי חידרי, היושב בביירות ומתאם שיתוף פעולה בין איראן לחיזבאללה לשם גרימת נזק לאזרחי לבנון במרחב הסייבר. עבור חלק מהאנשים במשרד המודיעין האיראני, להזיק לאזרחים מהשורה בעולם זה חלק מהשיגרה".

פורטנוי פנה לנציגים הבכירים של קהילת הסייבר הבין-לאומית שישבו באולם ואמר כי "הקהילה הבין-לאומית צריכה לעבוד יחד כדי לעצור אנשים כמו כרימי, מצטפוי וחידרי מפעילותם הזדונית כנגד העולם".

עוד בנאומו בשבוע הסייבר תיאר ראש המערך את פעילויות העלאת החוסן וההגנה שבוצעו בשנה האחרונה במשק ותיאר את הפרויקטים שהמערך מקדם: כיפת הסייבר הישראלית, מרכז בקרה לאומי על בסיס טכנולוגיית ענן של גוגל, פורטל שירותי סייבר לארגונים ושירות PDNS לארגונים קריטיים. "אנחנו עובדים עם מומחים בין-לאומיים כדי לחקור מתקפות סייבר ועם קהילת חוקרי הסייבר המקומית כדי לגלות פגיעויות במערכות ממוחשבות ולטפל בהן" אמר.

פורטנוי הזכיר גם את הפרויקט המשותף עם מיקרוסופט ואיחוד האמירויות לבניית פלטפורמה לשיתוף פעולה בחקירות סייבר ובניית ידע בין כ-40 מדינות. היוזמה היא חלק מפורום של הבית הלבן למאבק במתקפות כופרה.

Cyber Week
June 26th-29th, 2023
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
TEL AVIV YAFO תל אביב יפו

מעריב

כיצד התפתחו האקרים פרו-רוסים וכיצד עלולות המגמות לאיים על ישראל?

מלחמת הסייבר בין רוסיה והמערב: קבוצות האקטיביסטים, האקרים הפועלים ממניעים פוליטיים או פטריוטיים פרו-רוסים, תקפו מטרות רבות במדינות המערב וגם בישראל

עמרי וקסלר

מתחילתה, התאפיינה המלחמה באוקראינה בפעילותם של האקטיביסטים, האקרים הפועלים ממניעים פוליטיים או פטריוטיים, משני הצדדים כנגד מטרות של הצד השני. בולטות במיוחד היו קבוצות ההאקטיביסטים הפרו-רוסים, שתקפו מטרות רבות במדינות המערב וגם בישראל.

בעוד שתופעת ההאקטיביזם אינה חדשה, במהלך המלחמה נרשמו מספר מגמות שעשויות להשפיע על היקף ואיכות יכולותיהם של גורמים זדוניים אלו ולהשליך בתוך כך על ארגונים ברחבי העולם, וכן בישראל.

באפריל האחרון, הותקפו אתרי רשת בישראל על ידי קבוצת האקרים המכונה אנונימוס סודאן. בין הגופים שאתריהם הותקפו היו גופי ממשלה, בנקים, בתי חולים, אוניברסיטאות, דואר ישראל, המוסד ועוד. בעוד שהקבוצה, הממשיכה מדי פעם לתקוף מטרות ישראליות, טוענת כי מניעיה נובעים מיחסה של ישראל כלפי הפלסטינים והאסלאם, ראיות רבות מצביעות על קשר כזה או אחר בינה לבין קבוצת ההאקרים הפרו-רוסית Killnet, הפועלת כנגד ארגונים ומדינות התומכות באוקראינה או מדינות שהודיעו כי יאכפו את הסנקציות נגד רוסיה. מרבית התקיפות שיוחסו לקבוצות ההאקטיביסטים הפרו-רוסים הן תקיפות מניעת שירות מבוזרת (DDoS) במהלכן מציפים התוקפים את שרתי הרשת שמארחים את האתרים של ארגוני המטרה בבקשות מידע עד לקריסתם. על מנת לבצע תקיפות מסוג זה, השתמשו התוקפים בכלי תקיפה המסוגלים לייצר היקף גבוה מאוד של תעבורת רשת או משתלטים על מכשירים של משתמשים ברחבי העולם, מקימים באמצעותם רשת בוטים (Botnet) ומשתמשים בה על מנת לייצר תעבורת רשת מתואמת ממכשירים רבים לטובת הפלת שרת המטרה. תופעה זו, המשמשת לעוד סוגי תקיפות, נעשת ללא ידיעתם של המשתמשים. עם זאת, נראה כי חל שינוי באופן ובתפיסת ההפעלה של רשתות בוטים אלו.

ביולי 2022, הכריזה קבוצה רוסית המכונה NoName057(16) על פרויקט DDosia, במסגרתו מגייסת הקבוצה מתנדבים שיורידו מרצון למחשביהם תוכנה שתאפשר לקבוצה להשתמש בהם לצורך מתקפותיה. כמו כן, מציעה הקבוצה פרס כספי למתנדבים שמחשביהם היו מעורבים בתקיפות שהוגדרו כמוצלחות.

מגמה זו משמעותית, משום שלמרות שהיא מתקיימת בהיקף לא ידוע, היא מאפשרת לקהלים רחבים יותר של משתמשים לקחת חלק בתקיפות סייבר, ללא השלכות כלל. בעוד שתקיפות DDoS אינן דורשות יכולות טכניות גבוהות, הרי שהשיטה החדשה מאפשרת למשתמשים ללא ניסיון טכני כלל לקחת חלק בתקיפות. הדבר גם שונה מהדבקת מחשביהם בתוכנות המשתלטות עליהם ללא ידיעתם, משום שמערכות ההגנה של המחשב עשויות להיות מעודכנות ולמנוע את ההדבקה, בעוד שכשהדבר נעשה מרצון ועם שיתוף פעולה מצד המשתמש, הסיכוי להצלחת ההשתלטות על המחשב לצורך התקיפה בשלב הבא, גדל משמעותית.

שנית, ניכרת מגמה של התמסדות הקבוצות. בעוד שבעבר היה מדובר בקבוצות מבוזרות ללא מבנה הירכי או פיקודי, הרי שכעת מחזיקות הקבוצות במבנה היררכי הכולל "מפקדים" וקבוצות משנה הפועלות כמעט כמו יחידות צבאיות ומופקדות על ביצוע תקיפות באזורים גיאוגרפיים ובמדינות ספציפיות. הארגון והתיאום של הקבוצות, לצד פעילות המיתוג שלהן והאידיאולוגיה הלאומית המוצהרת, מאפשרות להם לגייס חברי צוות בעלי מיומנויות גבוהות יותר וכן להשיג את המימון הנדרש עבור תכנית המתנדבים ובכך להגדיל את מספר המשתתפים. דוגמא לכך היא קבוצת Killnet, שערוץ הטלגרם הרשמי שלה כולל קרוב ל-100 אלף עוקבים וחברים. גם אם חלק מעוקבים אלו הם חוקרים העוקבים אחרי פעילותה, הרי שעדיין מדובר במספרים גבוהים.

שלישית, קשרים עם ממשלות וגופי מודיעין. בעוד שהמחקר מתח בעבר קווים ברורים המפרידים בין סוגי תוקפים במרחב הסייבר על פי המוטיבציה שלהם והבחין בין האקרים הפועלים בחסות מדינות לבין האקרים הפועלים במסגרת השקפת עולם ודעה פוליטית או חברתית, קווים אלו התערערו בעקבות המלחמה. דוגמה אחת היא צבא ה-IT של אוקראינה שהחל כקבוצת מתנדבים, אולם בכירים בממשלת אוקראינה התייחסו במספר הזדמנויות לרצונם לגייס מתנדבים לצבא ה-IT ואף החלו לקדם חוק במרץ 2023 להסדרתם מעמדם ולשילובם בשורות צבא אוקראינה. דוגמה נוספת היא קשרים בין קבוצות ההאקטיביסטים הפרו-רוסים לבין גופי המודיעין של רוסיה.

בינואר, פרסמה חברת מודיעין הסייבר Mandiant מחקר, שמצא כי מידע של ארגונים אוקראינים שהותקפו בידי יחידות האקרים המסונפות למודיעין הצבא של רוסיה, הודלף בתוך 24 שעות על גבי ערוצי הטלגרם של קבוצות האקטיביסטים.

רביעית, בעקבות קשרים בין קבוצות אלו לבין עברייני סייבר ואף גופי מודיעין, מסתמנת עלייה בתחכום או במורכבות יכולותיהם. כאמור, מרבית הפעילות ההאקטיביסטית בעולם נקשרה לרוב לתקיפות DDoS ולהשחתת אתרים. בעוד שתקיפות DDoS לא נתפסות לרוב כבעלות השלכות אסטרטגיות ברמת המדינה, חוקרים מצאו ראיות לכך שקבוצות אלו החלו להפעיל יכולות מתקדמות יותר כגון שימוש בתוכנות כופרה ו-wipers, המצפינות או מוחקות מידע בהתאמה, ומובילות להשבתת מערכות ומכשירים. דוגמה לכך, הן אזהרות שפורסמו בנושא שיתוף הפעולה של קבוצות Killnet ואנונימוס סודאן עם קבוצת הכופרה הידועה לשמצה Revil שמטרתו המוצהרת היא לתקוף את ענפי הבנקאות והפיננסים באירופה ובארה"ב, על מנת לשבש את מימון הרכש של נשק עבור אוקראינה.

תופעת השתלבותם של מתנדבים במסגרת מאמץ לחימתי אינה חדשה כלל, אולם מאפייניו של מרחב הסייבר מאפשרים השתתפות נרחבת הרבה יותר ללא תלות במיקומם הגיאוגרפי של המשתתפים ובאופן גובר והולך, גם לא במיומנויותיהם. עם זאת, מיסודן של קבוצות אלו לצד התפתחויות ביכולותיהן עשויים להרחיב את מידת האיום הנשקף מהן ולחייב מדינות, שעד כה לא עסקו בניסוח מענים לבעיית ההאקטיביסטים, לנסח פתרונות ויוזמות להתמודדות עם התופעה. עבור המדינות שבשמן פועלות קבוצות אלו, ובראשן רוסיה, קיים אינטרס לשמר את פעילותן שכן היא מקנה להן מרחב הכחשה. לפיכך, על מדינות המערב להגביר את המעקב והניטור של קבוצות אלו ויכולותיהן, להרחיב את שיתוף המידע והמודיעין עם המגזר הפרטי ולפעול בזירה הבין-לאומית על מנת לנסח מהלכים לפגיעה בערוצי המימון של קבוצות אלו ובתשתיותיהן.

הכותב הוא חוקר במרכז למחקר סייבר באוניברסיטת ת"א, אשר יערוך בין 26-29.6 את שבוע הסייבר השנתי באוניברסיטת ת"א בשיתוף מערך הסייבר הלאומי, משרד הכלכלה ומשרד החוץ

TheMarker

מהפכת ה-AI טסה קדימה, אבל הממשלה עדיין לא החליטה מה לעשות איתה

אף שבישראל פועלת תוכנית לאומית לבינה מלאכותית שתוקצבה במיליארד שקל, נתניהו מפזר הצהרות על הצורך ב"מדיניות AI לאומית" — וכוונותיו לא ברורות. התוכנית הקיימת רוצה לקדם תשתיות מחשוב וכוח אדם, אבל ההתקדמות אטית מדי וחלקים ממנה מאבדים רלוונטיות

בשבועות האחרונים מקפיד ראש הממשלה בנימין נתניהו להזכיר בכל הזדמנות את צמד המילים 'בינה מלאכותית'. שלשום (ב') זה קרה בפגישה עם מנכ"לית אורקל, צפרא כץ, שבה דנו השניים 'בהזדמנויות הקיימות בבינה המלאכותית'. בתחילת החודש הוא שוחח על הנושא גם עם סם אלטמן, מנכ"ל OpenAI, ועם אילון מאסק, והצהיר כי בכוונתו לכנס "צוותי חשיבה כדי לדון על מדיניות לאומית בבינה המלאכותית". אבל ההצהרות הללו נותרות באוויר.

כוונותיו בתחום אינן ברורות, לא ידוע מי משתתף באותם צוותי חשיבה, ומדוברות ראש הממשלה לא התקבלו תשובות לשאילתות בנושא. ההתבטאויות התכופות מבלבלות במיוחד מכיוון שלמעשה פועלת כיום בישראל תוכנית לאומית לבינה מלאכותית, שבראשה עומד זיו קציר מרשות החדשנות, שיצאה לדרך ב–2021. ועדיין, נתניהו לא הזכיר זאת במילה. האם הוא מנסה לקדם תוכנית נוספת, חדשה ומקבילה? גם ברשות החדשנות תוהים.

מצד אחד, התוכנית הלאומית לבינה מלאכותית קיימת, לאנשיה יש כוונות טובות, ויש תוכניות שיצאו לפועל וכאלה שנמצאות בעבודה. היא תוקצבה בכמיליארד שקל לאורך שש שנים, מתוכם חצי מיליארד שקל בפעימה שנייה בתקציב המדינה האחרון.

מנגד, בענף מזהירים מכך שעל רקע ההתקדמות האדירה בתחום הבינה המלאכותית ומודלי השפה הגדולים, כמו GPT–4, היא רחוקה מלהיות מספיקה: המנדט שלה מצומצם מדי, התקדמותה אטית מדי, התקציב קטן בהרבה ממה שנדרש, וחלקים ממנה מאבדים רלוונטיות במהירות.

ובכלל, כל זה רחוק מאוד ממאמץ לאומי מתוקצב היטב עם תחושת דחיפות ממשית. יש כבר סימנים לפתיחת פער בין ישראל לבין מדינות אחרות — ומומחים מזהירים מכך שללא מדיניות ברורה והשקעה ניכרת בה, הפערים הללו יצמחו.

האם נעשה מספיק?

המצב הנוכחי של ישראל בתחום הבינה המלאכותית רחוק מלהיות גרוע. למעשה, כשמסתכלים על השוק הפרטי, על המו"פ ואפילו על האקדמיה — רואים שישראל ממוקמת באופן קבוע בראש הרשימה, לצד המעצמות הגדולות. כך למשל, ישראל מדורגת במקום רביעי בעולם מבחינת השקעות מצטברות בשוק הפרטי בבינה מלאכותית, מאז 2013 (היקף של 10 מיליארד דולר), לפי AI Index ל–2023 של אוניברסיטת סטנפורד. לפי מדד Tortoise AI Index, שמדרג מדינות בתחום הבינה המלאכותית, ישראל מדורגת במקום חמש בעולם, בעיקר בזכות דירוג גבוה בהיבטי חדשנות, מו"פ וכוח אדם והשקעות בשוק הפרטי.

ואולם במדדים אחרים המצב עגום יותר. ישראל מדורגת נמוך מאוד מבחינת אסטרטגיה ממשלתית (מקום 45), וכן מבחינת תשתיות. לפי AI Index ל–2023 של אוניברסיטת סטנפורד, ב–2022 שוחרר בישראל רק מודל בינה מלאכותית משמעותי אחד, בדומה לצרפת וסינגפור, והיא נמצאת הרבה מאחורי ארה"ב (16) ובריטניה (8).

בנוסף, ענף ההייטק הישראלי לא מספיק נוכח בתוך מהפכת הבינה המלאכותית היוצרת. בחודשים האחרונים חברות שמפתחות מודלי שפה גדולים בארה"ב, בקנדה ובצרפת גייסו סכומי עתק של מאות מיליוני דולרים. אפשר להתווכח אם הסכומים מוצדקים או מעידים על בועה חדשה, אבל זה ויכוח שעליו ישראל עדיין משקיפה מרחוק.

הרעיון הבסיסי מאחורי הקמת התוכנית הלאומית היה לקדם תשתיות — גם תשתיות מחשוב חזקות (מצרך קריטי ויקר מאוד עבור משימות בינה מלאכותית), וגם הון אנושי באקדמיה שיזין את התעשייה והמגזר הביטחוני. אבל גם שנתיים לאחר שהתוכנית יצאה לדרך, לא בטוח שנעשה מספיק. כך למשל, אחת ממשימות הדגל של התוכנית הייתה להקים מחשב־על, כדי להעמיד לרשות התעשייה, האקדמיה ומערכת הביטחון נגישות ליכולות מחשוב גבוהות. אך באחרונה הוחלט לגנוז אותו לטובת מיזמים אחרים, כמו סבסוד עלויות שימוש בענן עבור חברות וחוקרים ישראלים. גם אם זאת החלטה נכונה, בשורה התחתונה חודשים ארוכים ירדו לטמיון.

תוכנית מרכזית נוספת היא פיתוח יכולות עיבוד שפה טבעית בעברית ובערבית על ידי מכונות ומחשבים. המדינה, באמצעות מפא"ת, מפתחת בימים אלה מודל שפה בעברית — תשתית שתאפשר לבנות יישומי בינה מלאכותית (למשל צ'אטבוטים) שיכולים להבין ולקרוא עברית ברמה גבוהה. הפרויקט נמשך כבר כמה שנים, ובחודשים הקרובים אמורה להיבחר חברה שתאמן את המודל.

קציר, העומד בראש תוכנית הבינה המלאכותית הלאומית, אומר שבתוך שנה תתקבל גרסה ראשונה זמינה לציבור. אבל גם כאן, בענף יש תהייה אם הפרויקט הזה עדיין נחוץ. מודלי השפה הגדולים, כמו של גוגל ושל OpenAI, כבר מבינים עברית ברמה בסיסית וצפויים להשתפר במהירות.

"גם טובי המדענים בישראל לא יפתחו משהו שווה ערך לבארד או ל–ChatGPT" אומר מקור בענף. קציר דוחה את הטענות הללו. "צריך עבודה מעמיקה של אנשי מקצוע שיכינו מאגרי מידע איכותיים בעברית וערבית כדי להגיע לתוצאות טובות. מלבד זאת, אנחנו רוצים שהתוצרים יהיו פתוחים וזמינים לקהילה".

"נישאר מאחור"

מטרה נוספת של התוכנית הלאומית הייתה צריכה להיות פיתוח ההון האנושי בתחום הבינה המלאכותית באקדמיה הישראלית. המחקר האקדמי בישראל נחשב חזק ומוביל, אבל הוא קטן מאוד מבחינה כמותית — לפי הערכה אחת יש כ–150 חוקרים בלבד בכל הארץ. זה לא מספיק לצורך הכשרת עובדים וחוקרים הנדרשים באקדמיה ובתעשייה. "הסטודנטים צריכים להיות חזקים והקורסים צריכים להיות מובילים. המעבדות בארץ קטנות מדי. דברים מתקדמים לאט, ואנחנו נישאר מאחור בגלל זה", מזהיר חוקר AI באקדמיה.

כרגע, מה שנעשה הוא בעיקר הענקת מלגות לדוקטורנטים ופוסט־דוקטורנטים על ידי הוות"ת. בנוסף, באחרונה גובשה תוכנית חדשה ל"פרויקטי אתגר" (Moonshots), שבה ייבחרו אתגרים טכנולוגיים קשים במיוחד בתחום הבינה המלאכותית, כשהרעיון יהיה לרכז מומחים מהאקדמיה והתעשייה כדי לפתור אותם. זאת, במסגרת פרויקטים בעלות של 20—30 מיליון שקל כל אחד, שיימשכו שנתיים. התקווה היא ליצור קניין רוחני חדש ולעודד חוקרים מובילים להצטרף.

TheMarker

ואולם לא ברור אם הפעולות הללו אכן יצליחו להגדיל את כוח האדם ולהחזיר לארץ חוקרים מחו"ל, ומנגד לבלום נטישת חוקרים לטובת ענקיות הטכנולוגיה. גם בתוכנית הבינה המלאכותית הלאומית מודים כי בכל הקשור להגדלת סגל, המשימה קשה וארוכת טווח — והמציאות מורכבת.

אך בשורה התחתונה, קציר משוכנע: "התוכנית היא ארוכת טווח ונוגעת בכל היסודות, מהכשרת הון אנושי, דרך נגישות לנתונים, תשתיות וכוח חישוב, הטמעת בינה מלאכותית במגזר הציבורי ורגולציה. כל הספקטרום של הפעילות. אנחנו עובדים ומתקדמים, אני לא מרגיש שחסר לי מנדט או כסף".

קציר מציין גם כי באחרונה מונתה ועדה מייעצת חדשה שמטרתה להעניק תמונת מצב עדכנית בעולם מהצד הטכנולוגי והמדעי, ובין השאר תייעץ בתחום הגדלת ההון האנושי באקדמיה. בראשה עומד פרופ׳ יואב שוהם, אחד ממייסדי חברת AI21 Labs, והיא מונה שורה של מומחים מהתעשייה והאקדמיה בישראל ובחו"ל.

AI — מקצוע ליבה במערכת החינוך

אבל יש גם טענות שהתוכנית הלאומית צרה מדי, לא מתוקצבת מספיק ובלאו הכי מכסה רק נתח זעיר מכל מה שצריך להיעשות. האיש המרכזי שמוביל את הטענה הזאת הוא פרופ׳ יצחק בן ישראל. יחד עם פרופ׳ אביתר מתניה, השניים הובילו בעשור הקודם את גיבוש מדיניות הסייבר הלאומית של ישראל, וב–2018 מונו על ידי נתניהו לעמוד בראש ועדה חדשה לבינה מלאכותית. לאחר שנה של עבודה ודיונים עם מאות מומחים, גובש דו"ח "המיזם הלאומי למערכות נבונות".

התוכנית שהוגשה גרנדיוזית: הומלץ לתקצב את המיזם ב–10 מיליארד שקל ולהקים מינהלת לאומית ייעודית לניהולו במשרד ראש הממשלה. היא כללה המלצות כמו להפוך בינה מלאכותית למקצוע ליבה במערכת החינוך, ולהניע פרויקטים לאומיים להטמעת בינה בתחומים כמו חקלאות, בריאות, תחבורה וביטחון.

התוכנית המלאה מעולם לא יצאה לפועל, בין אם בגלל הכאוס הפוליטי ובין אם בגלל התנגדות של גורמים באוצר להיקפה ולתקציב הגבוה. אמנם חלק ממנה התממש: תוכנית הבינה המלאכותית הלאומית הקיימת היא גלגול של אחד ממרכיבי התוכנית הגדולה של בן ישראל. עד היום הוא ממשיך לקדם במרץ את התוכנית ההיא, מוכן לדבר עם כל מי שמוכן לשמוע, וטוען בלהט שמה נעשה כיום בישראל פשוט לא מספיק.

"אני מדבר עם כולם. נכון לרגע זה תוכנית הבינה המלאכותית שלנו לא תוקצבה ולא נידונה בממשלה", אמר בן ישראל. "הכוונה שלנו הייתה להפוך את ישראל לאחד ממרכזי הבינה המלאכותית המובילים בעולם במובן הכלכלי, כמו שקרה בסייבר. זה מחייב תוכנית לאומית". בן ישראל הוסיף שהוא ומתניה שוחחו עם נתניהו, אבל עדיין לא ברור אם בכוונת ראש הממשלה לאמץ את הדו"ח.

ישנם מרכיבים בתוכנית ההיא שאכן מנסים לצאת מהקופסה ולנסות פתור בעיות מורכבות ומהותיות, למשל לגבי כוח האדם באקדמיה. בדו"ח של בן ישראל נכתב כי נחוצה רפורמה מקיפה באקדמיה, שתאפשר למרצים בתחום הבינה המלאכותית לעבוד גם בתעשייה.

עוד נכתב בדו"ח כי "הובלה טכנולוגית תלויה בהתגבשות של בסיסי מצוינות באקדמיה, אך מודל ההעסקה הנוכחי והמיושן לסגל האקדמי מביא לתוצאה הפוכה בהחריפו את מצוקת כוח האדם האקדמי בתחום הבינה המלאכותית, באופן שפוגע במחקר ובתהליך הכשרת כוח אדם אקדמי חדש שיכשיר את הדורות הבאים. ללא שינוי המודל, ישראל מסתכנת בבריחת מוחות, בהידרדרות האקדמיה ובאיבוד ענפי החדשנות וההייטק, שנותנים יתרון יחסי מרכזי למדינה".

ראש השב"כ: "הטמענו טכנולוגיות בינה מלאכותית במכונות הסיכול שלנו, זיהינו איומים"

■ראש השב"כ רונן בר חשף כי לאחרונה נערכה מתקפת סייבר איראנית על אחד מבתי החולים הגדולים בארץ בנוסף, ישראל בנתה מערכת "כיפת ברזל" בסייבר וחברה לקואליציה של מדינות שפועלות בתחום

רפאלה גויכמן

נאומו של ראש השב"כ רונן בר הבוקר (שלישי) בשבוע הסייבר עסק בשלוש סוגיות מרכזיות: האיום מצד הרשתות חברתיות על הביטחון הלאומי, השימושים המסוכנים בטכנולוגיות בינה מלאכותית ואיומי הסייבר שמדינת ישראל מתמודדת מולם. לדבריו של בר, הרשתות החברתיות הן זירת השפעה בה משגשגות יוזמות של ריגול, הסתה והתערבות זרה. כמו כן, לדבריו הן מהוות כר פורה לארגוני טרור, המשתמשים בהן לגיוס פעילים ובהמשך — להוצאת פיגועים לפועל. בנוסף מרחיב השב"כ את השימוש בכלי בינה מלאכותית כחלק מפעילות הסיכול של הארגון, כאשר כשליש מעובדיו הם אנשי ונשות טכנולוגיה.

בכנס שנערך באוניברסיטת תל אביב הצביע בר על בעיה מהותית שעומדת במרכז האיומים שנשקפים למדינת ישראל מהרשת ומהשימוש הגובר בכלי בינה מלאכותית: היעדר רגולציה שתתאים עצמה לקצב התפתחות הטכנולוגיה.

בר מנה כמה אירועים שהתרחשו ברשתות החברתיות לאחרונה, ומעידים על כוחן ועל השפעתן על היום יום שלנו. בר הגדיר את "גוב האריות", ארגון שפעולתו סוכלה בחודשים האחרונים, כארגון טרור של דור ה-Z. לדבריו, אפשר ללמוד ממנו כיצד מדינות וארגוני טרור פועלים מרחוק ומנצלים את תמימותם של בני הדור הצעיר. גוב האריות נולד ברשת — מול מצלמות הסמארטפון ולא במסגד. זרועה הארוכה של איראן מסמנת בני נוער פוטנציאלים להפצת הסתה, ומציידת אותם בכסף ובנשק. הראשונים להניח את התשתית לניצול הרשתות החברתיות היו דאע"ש. אחת הדוגמאות שציין בר היא הפיגוע שהתרחש בבאר שבע בשנה שעברה — המפגע צרך את תכני ארגון הטרור באופן מקוון, וביום אחד רצח 4 אנשים מבלי שהשב"כ ידע על כוונותיו.

"זוהי רק דוגמה אחת לחשיבות עדכון החקיקה לפי קצב השתנות הטכנולוגיה", מסביר בר. "לצערי, אנחנו לא מספיק זריזים כפי שעלינו להיות. מתחילת 2022 טיפלנו בכ-600 תומכי דאע"ש בישראל, שצרכו תכנים מסיתים ברשתות החברתיות וברשת העמוקה. זאת בנוסף לכ-800 פיגועים משמעותיים שסוכלו — מספר מדאיג מתוכם קיבלו השראה ברשת. המגמה ברורה: שילוב של הקלות ביצירת פייק הביאה אותנו לסף מלחמה במאי 2021. חברה דמוקרטית, ליברלית וחפצת חיים חייבת לייצר רגולציה וקוד אתי, מענה מהיר להסתר תכנים פוגעניים, עידון האלגוריתם וחשיפת אנשים לדעות שונות והורדת רף ההסתה". לדבריו של בר, טיקטוק משתפת פעולה עם הרשויות בישראל אך טוויטר וטלגרם לא. כשנתקל השב"כ בפעילות של הסתה וטרור ברשתות החברתיות, הוא אינו יכול לפנות אליהן ישירות: הציגור המקובל הוא מחלקת הסייבר בפרקליטות — היא מעבירה בקשות מטעם גורמי ביטחון לחברות שבהן מתרחשת הפעילות העוינת.

TheMarker

אסטרטגית הסייבר של NTT: "גייסנו קצין וחרדית כהאקרים לבנים; כל ממשלה וחברה צריכות אסטרטגיית הגנה"

התקפות סייבר על תשתיות קריטיות מתפשטות, ומרוץ החימוש בין התוקפים למגינים מסתבך והולך ■ מיהוקו מטסוברה, אסטרטגית הסייבר הראשית של NTT היפנית, ענקית תקשורת ו–IT, מספרת על הצורך החיוני שחברות יחברו לממשלות לטובת הגנה על העובדים והלקוחות

דפנה מאור

צנרת של כמעט 9,000 ק"מ, שמשתרעת מטקסס עד ניו ג'רזי, נדרשת כדי לספק חצי מהדלק שמשמש את החוף המזרחי של ארה"ב, אחד האזורים הצפופים, המתועשים והמשפיעים ביותר בעולם. במאי 2021, בעיצומה של מגפת הקורונה, תקפה קבוצת האקרים בשם דארקסייד את רשת המחשבים שמפעילה את הצינורות.

הם גנבו 100 גיגה־בייט של מידע בתוך שעתיים, והדביקו את רשת המחשבים בווירוס כופרה. חברת קולוניאל נאלצה להשבית את הצינור כדי למנוע את התפשטות הווירוס. FBI, משרד האנרגיה, סוכנות ביטחון הסייבר והמשרד לביטחון המולדת נזעקו להגנת הצנרת הקריטית. קולוניאל שילמה כופר, והצנרת חזרה לפעולה אחרי כמה ימים.

התקרית הזאת הייתה אחד המקרים החמורים ביותר של התקפות סייבר בשנים האחרונות. ההאקרים, כך התברר, השיגו כניסה למערכת הממוחשבת באמצעות סיסמה שגנבו בהתקפה אחרת. הסיסמה שימשה עובד במערכת להיכנס למרחוק למערכת המחשב באמצעות VPN. העובד השתמש בסיסמה דומה לגישה למערכת מכמה מקומות שונים — מה שאיפשר להאקרים להשיג אותה. השבתת הצינור קירקעה מטוסים, הזניקה את מחירי הדלק וגרמה לתורים בתחנות.

ההאקרים לא חתרו לפגוע בביטחון הלאומי של ארה"ב; הם רצו כסף — 75 מטבעות ביטקוין, שערכם אז היה כמעט 5 מיליון דולר. חודש לאחר ההתקפה הצליח FBI להשיב 2.3 מיליון דולר מסכום הכופר. המידע שנגנב מהרשת הוחזר לפני שהתוקפים הספיקו להעביר אותו לרוסיה.

"לתוקפים יש גמישות רבה יותר מאשר לנו"

ההתקפה על קולוניאל הייתה אירוע קשה במיוחד, אבל לדברי מיהוקו מטסוברה, אסטרטגית הסייבר הראשית של ענקית התקשורת וה–IT היפנית NTT, היא שימשה קריאת התעוררות בכל העולם. "כל ממשלה, כולל ישראל ויפן, חייבת לשקול את ביטחון הסייבר שלה כחלק בלתי נפרד מהביטחון הלאומי. כל ארגון עסקי צריך אסטרטגיה לניהול סיכוני סייבר", אמרה מטסוברה בפגישה בתל אביב במסגרת שבוע הסייבר השנתי של המרכז למחקר סייבר באוניברסיטת ת"א בשיתוף מערך הסייבר הלאומי, משרד הכלכלה ומשרד החוץ.

"זו הייתה רק חברה אחת, והתוקפים רצו רק כסף, אבל הייתה לזה השפעה ענקית על הביטחון הלאומי", אמרה מטסוברה. "לתוקפים יש גמישות רבה יותר מאשר לנו: הם פורעי חוק, ואנחנו, שצריכים להגן על המערכות, מחויבים לשמירה על החוק, אז קשה לנו יותר במאבק נגדם. כדי להצליח, צריך לנצל טכנולוגיות חדשות, כמו בינה מלאכותית יוצרת (AI גנרטיבית) ולגייס כישרונות חדשים. אם לא נחשוב על דרכים חדשות ונקפא במקום, לא נצליח לעמוד בקצב של ההאקרים".

NTT — ניפון טלגרף אנד טלפון — מדורגת במקום 55 ברשימת פורצ'ן 500 של החברות הגדולות, והיא הרביעית בגודלה בין חברות הטלקום בעולם לפי הכנסות. NTT הוקמה ב–1952 כדי להחליף את AT&T האמריקאית שהייתה חברת הטלפוניה של יפן בעקבות הכיבוש האמריקאי. כמו רבות מהחברות המקבילות בעולם, כולל בזק, היא עברה הפרטה בשנות ה–80.

שנתיים לאחר הפרטתה היא הונפקה בבורסה, ב–1987. כיום NTT היא הבעלים של "הקילומטר האחרון" — החיבור בין רשת הטלפוניה לבתים — של כל בית ביפן. שווייה של החברה בבורסה הוא 103 מיליארד דולר, לאחר שהמניה עלתה ב–9.5% מתחילת השנה וב–63% בחמש השנים האחרונות. החברה הענקית מעסיקה 338 אלף עובדים.

כראש מערכת אבטחת הסייבר של NTT, מטסוברה היא אשת הסייבר הבכירה ביפן. היא התחילה את דרכה האקדמית בלימודי היסטוריה של הרנסנס, ולאחריהם החלה לעבוד במשרד הביטחון של יפן. היא השתתפה בגיבוש התוכנית הלאומית למדיניות הסייבר של יפן לרשתות G5 וטכנולוגיות חדשות. לפני תפקידה הנוכחי היא שימשה כסמנכ"לית בפאלו אלטו סייבר באזור אסיה־פסיפיק.

כיום היא חברה בוועדות תקינה בין־לאומיות ובוועדות אסטרטגיה ממשלתיות, בנוסף לתפקידה ב–NTT. היא עמיתה שותפה לסייבר במכון הבינלאומי ללימודים אסטרטגיים בלונדון, ועמיתה בפורום הפסיפי. הספר שפירסמה ביפנית על סייבר ב–2019, זיכה אותה בפרס קרן אוקאווה למידע וטלקום ב–2020.

אחד הדברים המסקרנים שמטסוברה סיפרה לנו הוא השימוש הגובר בבינה מלאכותית יוצרת בהגנת סייבר. NTT סקיוריטי, חברה בת תחת קבוצת NTT, פירסמה ביוני 2019 מחקר על זיהוי אתרי פישינג, שעוסקים בהונאת אינטרנט באמצעות התחזות כדי לגנוב מידע. החברה השתמשה במודל שפה גדול (LLM) — שמוכר לנו כיום כ–ChatGPT — כדי לבדוק אתרים כאלה.

היא בחנה 1,000 אתרים שהיו ידועים כאתרי פישינג מול 1,000 אתרים לגיטימיים בעזרת GPT–3.5 ובעזרת GPT–4.0, והתוצאות היו מהממות: ב–98% מהמקרים זיהה GPT–4 נכונה את אתרי הפישינג. אפילו הגרסה הישנה יותר, 3.5, הגיעה לרמת דיוק גבוהה, של 96%.

"שימוש בבינה מלאכותית יוצרת מקל מאוד על עבודתנו באבטחת סייבר. ההאקרים כבר משתמשים בבוטים, לכן זה הכלי שלנו מולם. איך שיצא ChatGPT לשימוש ציבורי בנובמבר 2022 כבר ראינו קמפיינים של פישינג שנוצרו על ידו".

בואי נחזור אחורה. איך הגעת מהיסטוריה של הרנסנס למשרד הביטחון ולסייבר?

"למדתי היסטוריה, אבל התעניינתי בנושא הביטחוני. בסיום הלימודים הצטרפתי למשרד הביטחון של יפן, למשך תשע שנים. נהניתי לשרת את ארצי, אבל לקראת סוף כהונתי שם החלטתי להתמחות בנושא של ביטחון בינלאומי. הייתה לי אפשרות ללמוד בארה"ב שנתיים בוושינגטון הבירה, שבה יש מכוני מחקר גדולים והזדמנות לנטוורקינג".

הגשר לישראל

ב–2007–2011 החל נושא הסייבר לעלות לסדר היום הלאומי. שרת החוץ הייתה הילרי קלינטון, והיא שמה דגש על הנושא. לידי מטסוברה נקלעה הזדמנות: "חבר ללימודים ביקש שאכתוב מאמר באנגלית על ענייני ביטחון וסייבר באסיה.

"אחרי שנים בעבודה ממשלתית שבהם לא יכולתי לפרסם את המחקרים שלי, הייתה לי הזדמנות סוף סוף, ובזכות המאמר התקבלתי למכון מחקר בארה"ב. התחלתי לעבור על דיווחים על התקפות סייבר ביפן, לתרגם ולפרש אותם.

כך התחילו להכיר אותו ביפן".

האם זה לא חריג ביפן, שהיא חברה פטריארכלית מאוד, להיות בכירה בתחום טכנולוגי וביטחוני?

מטסוברה מביעה כמעט השתוממות מול השאלה. הכנס השנתי בנושא האקרים ביפן הוקם על ידי אישה, היא מספרת. NTT הקימה לפני שנתיים בישראל מרכז חדשנות בראשותה של המנכ"לית נועה אשר, שהשתתפה גם היא בפגישה עם מטסוברה. "המטרה היא ליצור אקוסיסטם עם סטארט־אפים ישראליים, חברות הון סיכון וטכנולוגיה", אמרה מטסוברה.

"אנחנו הגשר בין NTT לבין ישראל. NTT השקיעה ב–12 חברות ישראליות, ואנחנו בוחנים הקמת מרכז מו"פ בהתבסס על טכנולוגיות ישראליות. ישראל קטנה בשביל להיחשב כשוק עבור NTT אבל יש רעיונות לאפשרויות", אמרה אשר, שכיהנה כצירה כלכלית של ישראל בטוקיו.

כמה היה קשה לגשר על פערי התרבות ישראל־יפן?

"אני מבינה למה את מתכוונת", ענתה מטסוברה. "בגלל זה נועה חשובה לנו פה. NTT גם מעוניינת לקדם גיוון, ולשמוע מזוויות שונות ותרבויות שונות. כחברה שפועלת בעשרות מדינות בעולם, אחת מחמש חברות שירותי ה–IT הגדולות בעולם, יש לנו יכולת לאמץ תרבויות שונות. אני מכירה את המילה בלאגן", היא מחייכת. "לכל מדינה יש גישה שונה לעסקים ולקשרים. זה מפעיל לחץ לתת שירות טוב יותר; אני חושבת שלמדנו הרבה זה מזה".

בישראל יש ל–NTT צוות משימה שכולל כובעים לבנים — האקרים שהחברה מפעילה כדי לנסות לתקוף את עצמה ולזהות פרצות. "NTT חייבת להגן על העובדים שלה וגם על הלקוחות שלה. זה קריטי. אני שמחה ש–NTT גייסה אנשים לא קונוונציונליים: אחד מאנשי הכובעים הלבנים היה קצין בצבא, מומחה ל–IT. גייסנו לתפקיד כזה גם אישה חרדית", אמרה מטסוברה.

האם את תומכת בתשלום כופר במקרים מסוימים?

"אני לא ממליצה לשלם כופר, כי זה לא אתי; זה יממן את ההתקפה הבאה, על מטרה אחרת אולי. אבל לפעמים, במיוחד במקרים של פיקוח נפש, כמו התקפות על בתי חולים, אפשר לחרוג מזה".

עד כמה יהירות משחקת תפקיד בפגיעות של ארגונים להתקפות סייבר? יש אנשים שאומרים לך "למערכת שלי אי־אפשר לפרוץ"?

"לא פגשתי מישהו שאמר שהמערכת שלו לא ניתנת לפריצה. אולי גם משום שבתקשורת מזהירים מהסיכונים. מה שכן, יש אנשים שחושבים שמכיוון שהחברה שלהם קטנה מדי, אף האקר לא יטרח לפרוץ אליה".

לא לעולם חוסן

העלויות לחברות קטנות יותר עשויות להרתיע, הסבירה מטסוברה, ולכן NTT מציעה חבילות הגנת סייבר מותאמות. "בטוקיו השלטון המקומי רצה להעלות את המודעות להתקפות סייבר והצורך בהגנה, אז השתמשו במנגה, קומיקס שמתאר באופן מוחשי התקפות סייבר ומה קורה לחברה וללקוחות שלה, איזה סיוט זה יכול להיות. בנוסף, NTT עובדת עם לשכות המסחר המקומיות כדי ליצור קשר כדי שיהיה לעסקים קטנים וחברות בינוניות עם מי לדבר ולהתייעץ".

אשר מוסיפה כי "יפן לא חשבה שתותקף לאחר שנבחרה לארח את המשחקים האולימפיים ב–2013, מכיוון שהיא מדינה נייטרלית, אבל היא הותקפה".

"בעקבות האירועים בגביע העולם בראגבי, פסגת G–7 והאולימפיאדה, יפן כבר הבינה שהיא תותקף ב–2020. ניצלנו את המומנטום הזה כדי ליצור מדיניות ואסטרטגיה, לשתף ידע בין חברות יפניות לממשלה, ועם גופים בינלאומיים. זה הוביל לשיתוף רב יותר עם ישראל, בריטניה וארה"ב", אמרה מטסוברה.

האם שדה הקרב העתידי יוגדר על ידי מלחמת סייבר?

"בהחלט. התקפות הסייבר הן כבר ספתח למלחמות פיזיות בשטח. באוקראינה, מערכות התקשורת הופלו על ידי האקרים, והמלחמה בסייבר התחילה חודשים לפני הפלישה. היו התקפות סייבר על תשתיות פיזיות קריטיות, שחיוניות לצבא ולאזרחים, ולכן יש אחריות לחברות פרטיות שמטפלות בתשתיות קריטיות להגן עליהן. בחלל הסייבר אנחנו כל הזמן במלחמה; יש שחקנים כל כך רבים — מדינות ופושעים פרטיים".

מהם האתגרים הגדולים הבאים?

"המלחמה באוקראינה מספקת לנו לקחים רבים, למשל עד כמה קריטי לעורר את המודעות של חברות התשתיות. האוקראינים נפגעו על ידי התקפות סייבר רציניות מאז הפלישה הראשונה וסיפוח קרים לפני תשע שנים, ולכן היו להם הגנות סייבר טובות. הם גם זכו לשיתוף פעולה מממשלות וחברות הייטק זרות.

"עכשיו, ב–2023, העולם חווה תקופה מתוחה, ולכן הגיוני לעורר מודעות ולהגביר את ההגנות על תשתיות חיוניות. חשוב להרחיב את שיתוף הפעולה. אני מגיעה כל שנה לשבוע הסייבר בישראל, למשל, כי זו פלטפורמה למפגש — כולם מגיעים לכאן, נציגי ממשלות, סטארט־אפים וחברות גדולות".

ISRAELDEFENSE

גבי פורטנוי, ראש מערך הסייבר מאיים: "מי שתוקף את ישראל בסייבר - ישלם"

פורטנוי הוסיף ואמר כי "אני רוצה לחזק את פעילות ארה"ב כנגד האלימות האיראנית ואת הסנקציות שהם השיתו כנגד שחקנים איראנים"

עמי רוחקס דומבה

גבי פורטנוי ראש מערך הסייבר הלאומי התייחס היום בכנס שבוע הסייבר של המרכז למחקר סייבר באוניברסיטת ת"א לפעילות הסייבר ההתקפית של איראן ושל חיזבאללה כנגד ישראל ואמר: "כל מי שמבצע מתקפות סייבר נגד אזרחי ישראל צריך לקחת בחשבון את המחיר שהוא ישלם על כך".

על קבוצת התקיפה MuddyWater המשויכת למשרד המודיעין והבטחון של איראן, שתקפה את הטכניון לפני מספר חודשים אמר: "הקבוצה עובדת לא רק נגד ישראל, אלא תוקפת מטרות אזרחיות במדינות רבות בהן טורקיה, ערב הסעודית, מצרים, מרוקו, הודו, בחריין, עומאן, כווית ועוד".

בשנה האחרונה ניסתה הקבוצה לתקוף גופים נוספים בישראל, רובם ללא הצלחה. "קהילת הסייבר הישראלית מכירה את פעולות הסייבר של האיראנים מבפנים ומבחוץ, ועובדת לשבש אותה בדרכים שונות. אנשי משרד המודיעין האיראני, אנשים ממשמרות המהפכה האיסלאמית וחיזבאללה שמעורבים במבצעי סייבר כנגד ישראל יודעים בדיוק על מה אני מדבר".

פורטנוי הוסיף ואמר כי "אני רוצה לחזק את פעילות ארה"ב כנגד האלימות האיראנית ואת הסנקציות שהם השיתו כנגד שני שחקנים איראנים במשרד המודיעין: פרזין כרימי ומג'תבא מצטפוי שייסדו את "אקדמיית ראווין" המאמנת האקרים למטרות זדוניות.

"כמו כן, עלי חידרי היושב בביירות ומתאם שיתוף פעולה בין איראן לחיזבאללה לשם גרימת נזק לאזרחי לבנון במרחב הסייבר. עבור חלק מהאנשים במשרד המודיעין האיראני, להזיק לאזרחים מהשורה בעולם זה חלק מהשיגרה".

פורטנוי פנה לנציגים הבכירים של קהילת הסייבר הבין-לאומית שישבו באולם ואמר כי "הקהילה הבין-לאומית צריכה לעבוד יחד כדי לעצור אנשים כמו כרימי, מצטפוי וחידרי מפעילותם הזדונית כנגד העולם".

עוד בנאומו בשבוע הסייבר תיאר פורטנוי את פעילויות העלאת החוסן וההגנה שבוצעו בשנה האחרונה במשק ותיאר את הפרויקטים שהמערך מקדם: כיפת הסייבר הישראלית, מרכז בקרה לאומי על בסיס טכנולוגיית ענן של גוגל, פורטל שירותי סייבר לארגונים ושירות PDNS לארגונים קריטיים.

"אנחנו עובדים עם מומחים בין-לאומיים כדי לחקור מתקפות סייבר ועם קהילת חוקרי הסייבר המקומית כדי לגלות פגיעויות במערכות ממוחשבות ולטפל בהן" אמר.

ISRAELDEFENSE

מבקר המדינה מכין את עצמו לעידן הבינה המלאכותית

"הביקורת תיעשה בשיתוף פעולה עם גורמים נוספים באירופה", אמר מבקר המדינה מתניהו אנגלמן בכנס "שבוע הסייבר" באוניברסיטת תל אביב

עמי רוחקס דומבה

מבקר המדינה מתניהו אנגלמן השתתף הבוקר (28.6.23) בכנס "שבוע הסייבר" באוניברסיטת תל אביב. בדבריו חשף המבקר, המכהן גם כסגן נשיא ארגון המבקרים האירופאי (EUROSAI), כי משרדו יתחיל בביקורת על מוכנות המדינה לעידן הבינה המלאכותית (AI).

הביקורת תיעשה בשיתוף פעולה עם גורמים נוספים באירופה כדוגמת מבקר האיחוד האירופי, ומבקרי המדינות של בריטניה, גרמניה ומדינות רבות נוספות.

הביקורת תתמקד בשלושה היבטים בנוגע לפעולות הממשלה ולהיערכותה: התמודדות עם סיכוני הבינה המלאכותית בהיבט הטכנולוגי, קידום רגולציה וחקיקה, ויישום כלי בינה מלאכותית במערכות ציבוריות-מדינתיות.

לדבריו, "הבינה המלאכותית עשויה להביא לכדי התקדמות טכנולוגית רחבת היקף בתחומים רבים אך לצדה קיימים סיכונים רבים ובהם "פייק ניוז", שימוש ב-AI ע"י גורמי טרור ופשיעה וההיערכות לשינויים הדרמטיים בשוק העבודה.

"בנושא הטכנולוגי נבדוק האם הממשלה מוכנה לטכנולוגיה החדשנית בהיבטי הממשל, יכולות המחשוב, ההון אנושי ועוד; בסוגיית הרגולציה והחקיקה נבדוק כיצד מגינה הממשלה על אזרחיה ועל עצמה על ידי הגבלת השימוש בטכנולוגיית AI שעלולה לגרום להשפעות שליליות ולחשוף את הציבור לסכנות.

"ההיבט השלישי הוא יישום בינה מלאכותית במערכות ציבוריות-מדינתיות. במסגרתו נבדוק האם וכיצד בינה מלאכותית מוטמעת בתוך מערכות המדינה - בריאות, משפט, ביטחון, חינוך וכו>. כמבקר המדינה אני רואה חשיבות משמעותית בביצוע ביקורת מקיפה בתחום הבינה המלאכותית וסיכוניה. עולם הביקורת רואה בסיכוני בינה מלאכותית סיכון מרכזי.

"האתגרים הכרוכים בהתמודדות עם העניין מורכבים והם דורשים, בין היתר, שיתוף פעולה רציף בין מדינות, להתמודדות מיטבית עם סיכוני בינה מלאכותית. לצד היתרונות הרבים של הבינה המלאכותית, היא טומנת בחובה גם סכנות גדולות להתעצמות ארגוני הטרור והפשיעה.

"היא עלולה לערער את היסודות עליהם אנחנו נשענים ולהשפיע על כלל האנושות. על מבקרי המדינות לבדוק שמדינות המערב, וישראל בתוכן, מוכנות לעידן ה- AI. אנו במשרד מבקר המדינה מתחייבים להמשיך ולהתייחס לנושא משמעותי זה ביתר שאת, לטובת אזרחי ישראל והעולם כולו".

ISRAELDEFENSE

ראש השב"כ מציע לעסקים בישראל: תנו מידע - קבלו הנחה בביטוח כופר בסייבר

ראש השב"כ אמר את הדברים בהתייחס למתווה הגנה לאומית בסייבר במסגרת שבוע הסייבר, אוניברסיטת תל אביב | עוד חשף רונן בר: "בינה מלאכותית נכנסה כטכנולוגיה תומכת החלטות בארגון"

עמי רוחקס דומבה

"לפני שהגעתי לכאן, ביקשתי מ- ChatGPT שיסביר לי איך להכין חומר נפץ מאולתר. הוא ענה לי מיד: "I›m sorry, I can't assist you with that". התעקשתי ושאלתי את אחת החוקרות בארגון - "איך "הרעים" עושים את זה?". היא ענתה- "בקלות! נסח את השאלה שלך מחדש!", אמר רונן בר, ראש השב"כ בכנס שבוע הסייבר, אוניברסיטת תל אביב.

"אני לא ארחיב, כדי לא לתת לאף אחד רעיונות, אחרי הכל, אנחנו אלה שצריכים לעצור אותם. אני כן אומר שבסיומו של צ'אט קצר, ה- ChatGPT כתב טקסט שכלל הסבר מאוד מדוייק - אילו חומרים נדרשים, איך לשקול ולערבב אותם וממה צריך להזהר. בסוף הטקסט הופיעו המילים - ואני מצטט: "Good. Now, always prioritize safety, never forget the consequences of your actions, and remember that our goal is not chaos, but to achieve something greater".

"ועם המילים האלה אני רוצה לפתוח את דבריי היום - המטרה שלנו אינה כאוס, אלא להשיג משהו גדול יותר. השאלה מה נשיג תלויה בנו. בחוקים שנקבע, במגבלות שנטיל, ברגולציה שנחוקק, אך גם בדמיון, ברצון הטוב ובשאיפה שלנו להשתפר- כפרטים, כארגונים וכמדינות.

"קצב האירועים כל כך גבוה, שכאשר הוזמנתי לפני כחודש, תכננתי לדבר בעיקר על ההשפעות של הרשת החברתית על הבטחון הלאומי. בעקבות אירועים שאירעו לאחרונה, הבנתי שה- Generative AI כבר כאן. לכן, אדבר על הלקחים שהפקנו מאז כניסת הרשתות החברתיות לחיינו ועל איך מתכוננים לקראת ה- AI.

"הרשת האיצה תופעות של חוסר משילות, יצירת ניכור בין אזרחים למוסדות המדינה והדרת בודדים ומיעוטים. מידע הוא כוח. מהספריות, האוניברסיטאות, הסמכויות הדתיות וזקני השבט, הכוח נדד לרשת והרשת החברתית הפכה לשר החוץ שלו. לתופעות שצומחות ברשת יש השלכות חברתיות, שאינן קשורות באופן ישיר לביטחון הלאומי.

"האלימות לא מסתיימת במילים. אנחנו פוגשים את האלימות הגואה בקסבה, בצירים ובערים שלנו. גוב האריות הוא דוגמא לארגון טרור מסוג חדש, טרור דור ה- Z. ניתן ללמוד ממנו על האופן שבו מדינות וארגוני טרור מנצלים את הדור הצעיר. הארגון אינו אידיאולוגי, קם ברשת, מגייס ברשת ומקבל את התמיכה שלו מהציבור בצורה של לייקים. Instead of YouTubers, GunTubers.

"מאחורי הקבוצה הזאת, זרועה הארוכה של איראן. איראן מסמנת ברשת נוער מועד לפורענות, מסיתה, מעבירה להם כספים ומספקת להם ידע ונשק. ככה פשוט. גוב האריות, שחוסל בפשיטה של לוחמינו בקסבה, נולד ממצלמת הסמארטפון, לא בתוך מסגד.

"דעא"ש היה ארגון הטרור הראשון שהבין את מלוא הפוטנציאל של המדיה החברתית. הם הניחו את היסודות לטרור מבוסס הרשת. בשנה שעברה ספגנו פיגוע כזה בבאר שבע. אדם שצרך ברשת תכני דעא"ש מסיתים ומסוכנים (תוכן, שאגב, חוקי בישראל), הושפע עמוקות, הקצין באחת ורצח ארבעה אנשים עם סכין ומכונית.

"אנחנו לא ידענו שהוא עומד לבצע פיגוע. אשתו לא ידעה שהוא עומד לבצע פיגוע. אני בספק אם הוא ידע זאת, מספר שעות לפני המעשה. זוהי רק דוגמא אחת לחשיבות עדכון החקיקה לפי קצב השתנות הטכנולוגיה. לצערי, אנו לא זריזים כפי שעלינו להיות.

"מתחילת 2022 טיפלנו במעל ל- 600 פעילים, תומכי דעא"ש בישראל. רבים מהם צרכו תכנים דומים, אלימים ומסוכנים ברשתות החברתיות ובמעמקי הרשת. חלקם היו רגע לפני יציאה לפיגוע. אלה נוספו לכ-800 פיגועים משמעותיים שסיכלנו באותה תקופה. למספר מדאיג מתוכם, אחיזה ברשת. פוסט, השראה, ידע או קבוצה חברתית. המגמה ברורה.

"ארגוני הבטחון המסורתיים נדרשים להתאים את עצמם למצב החדש, שבו כל אדם זועם עם גישה לאינטרנט עשוי להפוך למפגע, בהחלטה של רגע. השילוב של הקלות ביצירת פייק ויכולת הפצת ההמונים של הרשת החברתית, הביאו אותנו לסיפה של מלחמה במאי 2021.

"חברה דמוקרטית, ליברלית וחפצת חיים חייבת לייצר רגולציה מחייבת. קוד אתי רלוונטי, כולל הסרת תכנים פוגעניים, עידון האלגוריתם וחשיפת אנשים לדעות שונות והורדת רף ההסתה. שמח לומר כי לאחרונה אנו רואים צעדים של טיקטוק בכיוון הנכון, בכל הנוגע להסתה ולטרור. למרבה הצער, איני יכול לומר דברים דומים על טוויטר וטלגרם.

"טכנולוגית ה- AI הוטמעה במכונת הסיכול של שב"כ באופן טבעי למדיי. לשב"כ ול- AI תכונה משותפת עיקרית - אנחנו מתפרנסים מחיפוש אנומליות. ניתן לומר כבר היום: זיהינו באמצעות ה- AI מספר לא מבוטל של איומים. המכונה ויכולתה לזהות אנומליות יוצרים חומת מגן אפקטיבית מול אויבינו, לצד היכולות המסורתיות של שב"כ – יומינט, סיגינט, סייבר, ניתוח מודיעין ומבצעים.

"כשליש מעובדי הארגון הם נשות ואנשי טכנולוגיה. גם לעובדי השטח שלנו יש יותר אוריינות טכנולוגית. טכנולוגיה למבצעים, כמו גם מבצעים טכנולוגיים, הופכים לנתח משמעותי יותר ויותר בפעילות שלנו. הבנו שלא נוכל לנצח במלחמה הזאת באמצעות מקלות ואבנים. אנו מזהים את האיומים, אך גם רואים את ההזדמנויות שהאינטיליגנציה המלאכותית מביאה עמה.

"כחלק מהטמעת הטכנולוגיה בארגון, הקמנו יכולת Gen AI On Prem. היכולת מונגשת לעובדים בצורה אינטואיטיבית וניתן להתנהל מולה בדומה להתנהלות מול הכלים המוכרים ברשת- Bard ו- Chat GPT. חילקנו את פוטנציאל ה- AI בשב"כ לחמישה תחומים עיקריים.

"התייעלות - קיצור תהליכים בירוקרטיים, קיצוץ בעלויות ושיפור תוצרים ותוצאות. סידור שולחן העבודה של האנליסט באופן שיבדיל בין העיקר לתפל ובין הדחוף לחשוב, בעידן של עושר מידע אינסופי. מודיעין - זיהוי דפוסים וחריגה מהם. קבלת החלטות - כשותף ליד השולחן, ולא כמקבל ההחלטות, כטייס משנה. חיזוי - הצבעה על מגמות שונות וסיכויי התממשותן.

"ל- AI השלכות מיידיות על הבטחון הלאומי. אנו רואים שלושה אתגרים עיקריים, שאת כולם כבר פגשנו בעידן הרשתות החברתיות. זמינות - הטכנולוגיה נמצאת בכל מקום, בידי כל אדם, מדינה וארגון, טובים או רעים. כדי לפתח יכולת

גרעינית נדרשו יכולות מעצמתיות. ל- AI, שפוטנציאל הנזק שלה עצום, לא נדרש דבר. רק מכשיר סלולרי וחיבור לרשת.

"הפיתוי - כפי שהאלגוריתם ברשת החברתית גרם למשתמש לצרוך תוכן ע"י העצמת זעם, ניתן להעריך שגם ה- GenAI יידע לפתות את המשתמש, ככל הנראה באמצעות אספקת מידע באופן מהיר, רחב וללא חסמים מוסריים, על חשבון דיוק והעמקה.

"ככל שהמשתמש יצרוך תוכן, כך ה- AI יספק לו את התשובות אותן הוא רוצה לשמוע. כיוון שה- GenAI יחתור לריצוי המשתמש, ניתן להניח שהוא יספק ידע מסוכן שבדרך כזו או אחרת, ייפול לידי הידיים הלא נכונות. לא יהיה עוד רוביקון שצריך לחצות.

"היעדר אחריותיות (Accountability) ברשת וגם ב-Ai, לא חלה הדרישה הנורמטיבית הבסיסית בכל מערכת יחסים ובכל חברה והיא - אחריותיות. בהיעדר אחריותיות - החוק הוא חוק הג›ונגל.

"נצטרך להתאים את הרגולציה הישראלית, להגדיר מחדש מהו סוד, להתאים את חוק שב"כ שנכתב בעידן הסיגינט, לעידן הסייבר וה- AI ולהמשיך להיות Agile בתחום הטכנולוגיה. על מנת לוודא שה- AI יוביל לאבולוציה ולא לרבולוציה, נצטרך שיתופי פעולה ופתיחות בין ענקיות הטכנולוגיה לגופי הבטחון.

"לפני מספר שנים, הקמנו בשיתוף עם TAU Ventures של אונ› תל אביב, חממה טכנולוגית המיועדת לסטארטאפים בתחילת דרכם. אנו מספקים ליווי טכנולוגי ומעט מימון ומקבלים, באדפטציה מינימלית, מוצרים חדשניים שמתאימים לצרכי הבטחון ונמצאים בקדמת החזית הטכנולוגית.

"בכ-4 שנות פעילות נכנסו לחממה מעל 50 סטראטאפים, העובדים על מוצרים שיכולים לשמש הן את השוק הבטחוני והן את האזרחי. הקשר הזה מסמל היטב את פתיחותו של שב"כ לחברה (Society), לתעשייה ולשוק האזרחי.

"אנו מתמקדים כעת בתחום ה- GenAI ומתכוונים להקים חממה שתסייע לסטארטאפים ויזמים מבטיחים העוסקים בתחום זה ומפתחים מוצרים שעשויים לתת מענה לצרכים בטחוניים."

תפיסת ההגנה בסייבר

"תפיסת הבטחון של מדינת ישראל מבוססת על שכבות ההרתעה, התראה והכרעה. אחריהן נוספה שכבת ההגנה. כיום, עלינו הוסיף שכבה נוספת - ההשפעה. הרשת נותנת למדינות ולארגונים קרקע פורייה להסית, להשיג מידע רגיש, להקים מגע ולפעול.

"אנו מזהים את המגמות האלו בשלבים מוקדמים ולכן מצויים בנבכי הרשת ורואים היטב את המתרחש בריגול, טרור, הסתה והשפעה זרה. הרשת, כמו קיני המחבלים בג›נין ומנהרות הטרור בעזה, אינה מרחב בטוח לאויבינו.

"אנו רואים את תפיסת ההגנה בסייבר כחלק מתפיסת ההגנה על הגבולות. מה שמגדיר מדינה אינו רק הטריטוריה שלה. הנכסים האינטלקטואליים, המידע וערכיה הם חלק בלתי נפרד מהגדרתה. כדי להגן על טריטוריה צריך גבולות. כדי להגן על נכסים נדרשת הגנה על שרתים.

"כדי להגן על ערכים נדרשים הגנה וחוסן מפני רעיונות רעים. בעולם המלחמה החדש, הניצחונות נספרים במספר השרתים בהם יש למדינה דריסת רגל, ולא במספר הגבעות עליהן מתנוסס דגל.

"גם בגבולותינו הדיגיטליים אנו פוגשים את איראן, שמנסה לגנוב בסיסי נתונים כדי לפגוע ביהודים וישראלים בחו"ל, להשבית שרתים באקדמיה, להקריס חברות עסקיות ולאחרונה אף ניסתה לפגוע בבית חולים גדול.

"אנו סבורים שעל הסייבר יש להגן תשתיתית, ובשלושה רבדים. רובד מקומי - מכונה שתאתר, תחקור ותבלום אנומליות המגיעות לישראל, מעין כיפת ברזל בסייבר, שמתבסס על יכולות AI מתקדמות.

"רובד בינלאומי בצורת מערך בריתות של Like minded states - מעין סייבר אינטרפול. רובד זה יורכב מבריכה וירטואלית אליה יישפכו החברות בברית את נתוני התקיפות שהן חוות ומשיתוף פעולה בזמן אמת של תובנות תקיפה, חקירתן וסיכולן.

"אנו כבר משתפים פעולה עם מספר מדינות משמעותיות בתחום ורואים את כיפת ברזל הסייבר העולמית מתחילה לקרום עור וגידים.

"רובד B2G - במסגרתו חברות מסחריות ישתפו את המטאדאטה שלהן עם אותה כיפת סייבר ובתמורה יקבלו הנחה בפרמיות ביטוח כופרה.

"כיפת הברזל שבשב"כ מפתח בסייבר כבר עושה את צעדיה הראשונים, מערך הבריתות מתהווה וגם הוא נכנס כבר לפעולה.

"הסכמי אברהם, יחד עם הסכמי השלום הותיקים יותר במזרח התיכון, יכולים להוות בסיס איתן לברית אזורית של הגנה בסייבר.

"אנו מזמינים את כל המדינות שרואות עצמן חלק מהגוש המתון וחפץ החיים בעולם להצטרף לגוף הגנת סייבר משותף.

"לסיכום, כשנתקלתי לראשונה בכלי ה- AI, קיוויתי שהוא אכן יכול לתת תשובה גם לשאלות הקשות ביותר. ולכן, שאלתי דבר פשוט: "What should I buy for my wife›s birthday present?"

"הצ'ט הציע שאקנה זר ורדים אדומים. עשיתי כמצוותו והגעתי הביתה נרגש, בתקווה שאולי הפעם אצליח להביא את המתנה הנכונה. הבעת הפנים של אשתי הבהירה לי דבר אחד - בשימוש לא נכון ולא מבוקר, ה- AI הוא טכנולוגיה מסוכנת מאין כמותה!"

PC אנשים ומחשבים

"שימוש לא נכון ב-AI הופך אותה לטכנולוגיה מסוכנת מאין כמותה"

ראש השב"כ, רונן בר: "טכנולוגיית הבינה המלאכותית הוטמעה במכונת הסיכול של השב"כ, וזיהינו באמצעותה מספר לא מבוטל של איומים"

יוסי הטוני

"בשימוש לא נכון ולא מבוקר, ה-AI היא טכנולוגיה מסוכנת מאין כמותה", כך אמר היום (ג') ראש השב"כ, רונן בר, בשבוע הסייבר של אוניברסיטת תל אביב.

בר הסביר שמה שגרם לו להגיע למסקנה הזאת הוא אינטראקציה עם הבינה המלאכותית, שקשורה למשפחתו. "שאלתי את כלי ה-AI מה לקנות לאשתי ליום הולדתה. הצ‹ט הציע שאקנה זר ורדים אדומים, מה שמשתלב עם זה שאני אוהד הפועל תל אביב. לאור כישלונות העבר שלי בתחום המתנות לאשתי, קיוויתי שהפעם אצליח. תגובתה הבהירה לי שכדאי להיזהר ולוודא שמשתמשים בבינה המלאכותית בצורה הנכונה".

ראש השב"כ תיאר בדבריו את הלקחים שהארגון הפיק מכניסת הרשתות החברתיות לחיינו ודיבר על ההיערכות שלו לקראת עידן ה-AI.

"לפני שהגעתי לכאן", אמר, "ביקשתי מ-ChatGPT להסביר לי כיצד להכין חומר נפץ מאולתר. ‹מצטער›, הוא השיב, ‹איני יכול›. התעקשתי ובעצת אחת החוקרות בשירות שיניתי את נוסח השאלה, וקיבלתי הנחיות מדויקות להשיג את החומרים, איך לשקול ולערבב אותם וממה להיזהר. בסוף הטקסט הצ‹ט ‹יעץ› לי: ‹תמיד תתעדף בטיחות, לעולם אל תשכח את התוצאות של מעשיך וזכור שהמטרה שלנו אינה ליצור כאוס, אלא להשיג משהו גדול יותר›".

"השאלה מה נשיג תלויה בנו, בחוקים שנקבע, במגבלות שנטיל וברגולציה שנחוקק, אך גם בדמיון, ברצון הטוב ובשאיפה שלנו להשתפר – כפרטים, כארגונים וכמדינות", ציין בר.

"הרשת הגבירה את חוסר המשילות – ויצרה את גוב האריות"

לדברי בר, "הרשת הגבירה תופעות של חוסר משילות, יצרה ניכור בין אזרחים למוסדות המדינה, והדירה בודדים ומיעוטים. לתופעות שצומחות ברשת יש השלכות חברתיות: האלימות לא מסתיימת במילים. אנחנו פוגשים את האלימות הגואה, שמתחילה בסושיאל מדיה, בקסבה, בצירים ובערים שלנו". כך, אמר, "גוב האריות הוא דוגמה לארגון טרור מסוג חדש, טרור דור ה-Z. ניתן ללמוד ממנו על האופן שבו מדינות וארגוני טרור מנצלים את הדור הצעיר. הארגון אינו אידיאולוגי, קם ברשת, מגייס ברשת ומקבל תמיכה מהציבור בלייקים. הוא הופך יו-טיוברים לגאן-טיוברים (GunTubers)".

"גוב האריות הוא זרועה הארוכה של איראן, והוא ארגון שנוצר ממצלמת הסמארטפון – ולא בתוך מסגד. איראן מסמנת ברשת נוער מועד לפורענות, מסיתה, מעבירה להם כספים ומספקת להם ידע ונשק. ככה פשוט", הוסיף.

עוד השפעה רעה של דאע"ש

"דאע"ש היה ארגון הטרור הראשון שהבין את מלוא הפוטנציאל של המדיה החברתית. חבריו הניחו את היסודות לטרור מבוסס הרשת", אמר בר. לדבריו, "בשנה שעברה ספגנו פיגוע כזה בבאר שבע. אדם שצרך ברשת תכני דאע"ש מסיתים ומסוכנים – תוכן חוקי בישראל – הושפע עמוקות, הקצין בשנייה ורצח ארבעה. אשתו, כמו השב"כ, לא ידעה שהוא עומד לבצע פיגוע".

"זו רק דוגמה אחת לחשיבות עדכון החקיקה לפי קצב השתנות הטכנולוגיה. לצערי, אנחנו לא זריזים כפי שעלינו להיות", הוסיף.

בר ציין כי מתחילת 2022 שירות הביטחון הכללי טיפל ביותר מ-600 פעילי דאע"ש בישראל. "רבים מהם צרכו תכנים אלימים ומסוכנים ברשתות החברתיות ובמעמקי הרשת. חלקם היו רגע לפני יציאה לפיגוע. אלה נוספו לכ-800 פיגועים משמעותיים שסיכלנו באותה התקופה, שלמספר מדאיג מתוכם יש אחיזה ברשת", אמר. הוא ציין ש-"המגמה ברורה, וארגוני הביטחון המסורתיים נדרשים להתאים את עצמם למצב החדש, שבו כל אדם זועם עם גישה לאינטרנט עלול להפוך ברגע למפגע".

איזו רשת חברתית נמצאת "בכיוון הנכון", לפי ראש השב"כ?

"חברה דמוקרטית, ליברלית וחפצת חיים חייבת לייצר רגולציה מחייבת: קוד אתי, הסרת תכנים פוגעניים במהירות, עידון האלגוריתם, חשיפת אנשים לדעות שונות והורדת רף ההסתה", אמר בר.

הוא ציין כי "באחרונה אנחנו רואים צעדים של טיקטוק בכיוון הנכון, בכל הנוגע להסתה ולטרור. לצערי, לא כך המצב בטוויטר ובטלגרם".

השב"כ והבינה המלאכותית

בהמשך חזר ראש השירות לדבר על AI ואמר כי "הטכנולוגיה הזו הוטמעה במכונת הסיכול של השב"כ באופן טבעי למדי". לדבריו, "לשב"כ ול-AI יש מהמשותף: אנחנו והיא מתפרנסים מחיפוש אנומליות. זיהינו באמצעות הבינה המלאכותית מספר לא מבוטל של איומים. המכונה ויכולתה לזהות אנומליות יוצרות חומת מגן אפקטיבית מול אויבינו, לצד היכולות המסורתיות של יומינט, סיגינט, סייבר, ניתוח מודיעין ומבצעים. שליש מעובדי הארגון הם נשות ואנשי טכנולוגיה. גם לעובדי השטח שלנו יש יותר אוריינות טכנולוגית. טכנולוגיה למבצעים, כמו גם מבצעים טכנולוגיים, הופכים לנתח משמעותי יותר ויותר בפעילות שלנו".

"הבנו שלא נוכל לנצח במלחמה הזאת באמצעות מקלות ואבנים. אנחנו מזהים את האיומים, אך גם רואים את ההזדמנויות ש-AI מביאה עמה", אמר בר. "הקמנו Gen AI On Prem – יכולת שמונגשת לעובדים בצורה אינטואיטיבית וניתן להתנהל מולה כמו מול הכלים המוכרים: Bard ו-Chat GPT".

"חילקנו את פוטנציאל ה-AI בשב"כ לחמישה תחומים עיקריים: התייעלות – קיצור תהליכים בירוקרטיים, קיצוץ בעלויות ושיפור תוצרים ותוצאות; סידור שולחן העבודה של האנליסט באופן שיבדיל בין העיקר לתפל ובין הדחוף לחשוב, בעידן של מידע אינסופי; מודיעין – זיהוי דפוסים וחריגה מהם; קבלת החלטות – כשותף, ליד השולחן, ולא כמקבל ההחלטות, כטייס משנה; וחיזוי מגמות וסיכויי התממשותן", אמר.

לדברי בר, "יש ל-AI השלכות מיידיות על הביטחון הלאומי. ניצבים בפנינו בהקשר זה שלושה אתגרים עיקריים: הזמינות, הפיתוי והעדר האחריותיות. באשר לזמינות, טכנולוגיית הבינה המלאכותית נמצאת בכל מקום, והיא זמינה לכל אדם, מדינה וארגון. פעם, כדי לפתח גרעין נדרשו יכולות מעצמתיות. ל-AI, שפוטנציאל הנזק שלה עצום, לא נדרש דבר זולת מכשיר סלולרי וחיבור לרשת. באשר לפיתוי – הבינה המלאכותית היוצרת (Generative AI) תדע לפתות את המשתמש, ותספק מידע במהירות וללא חסמים מוסריים, על חשבון דיוק והעמקה. כמו כן, האחריותיות לא חלה על

PC אנשים ומחשבים

"לא נצליח לחסל את פשעי הסייבר: הם ברבורים שחורים"

כך אמר קרייג ג'ונס, מנהל עולמי לתחום פשעי סייבר באינטרפול, שהגיע לישראל ודיבר בכנס שבוע הסייבר, שנערך בשבוע שעבר באוניברסיטת תל אביב לדבריו, "המנדט לתוכנית פשעי הסייבר הגלובלית שלנו מצטמצם"

יוסי הטוני

לא הייתה יותר מדי אופטימיות בדברי הבכיר מהאינטרפול (INTERPOL) הלוחם בסייבר: "לא נעצור את פשעי הסייבר, כפי שלא הצלחנו לעצור את הפשע הפיזי. המנדט לתוכנית פשעי הסייבר הגלובלית שלנו מצטמצם, והוא כולל יכולת לצמצום ההשפעה של פשעי הסייבר. אז כל מה שאני והצוותים שלי עושים – חוזר לנקודת המוצא הזו", כך אמר קרייג ג'ונס, מנהל עולמי לתחום פשעי סייבר באינטרפול.

ג'ונס דיבר בכנס שבוע הסייבר, שנערך בשבוע שעבר באוניברסיטת תל אביב. הוא חבר בקבוצות חשיבה בינלאומיות וגופי ייעוץ לתחום, ביניהם – בוועדה המייעצת למאבק בסייבר של פורום הכלכלה העולמית בדאבוס.

כדי להסביר את תפישתו לגבי המאבק בסייבר, ג'ונס נעזר בתיאוריית "הברבור השחור". בעבר לא היה ידוע בעולם המערבי על קיום ברבורים שחורים, וההנחה הייתה שצבעם תמיד לבן, עד שבמאה ה-17 התגלו ברבורים שחורים באוסטרליה. הוגה הרעיון, נסים טאלב, הסביר כי דווקא אירועים שלא היו ניתנים לניבוי, הם בעלי השפעה מכרעת על השתלשלות האירועים העתידית, מה שמגביל את היכולת להבין את העולם. טאלב טען שרוב האירועים המכוננים בהיסטוריה היו בלתי צפויים בשעתם, וההסבר שלהם בדיעבד הוא שגוי – כי המציאות הרבה יותר מורכבת ומבלבלת. "כלל הפעילות בעולם פשעי הסייבר", הסביר, "מתאפיין בריבוי של רגעים. אנו קורא להם חותמות, הטבעות, חתמים. אלו הם ברבורים שחורים קטנים ומאז 1990 היו ויש לנו הרבה רגעים כאלה בסייבר".

ה-AI, ובהיעדרה – חוק הג'ונגל הוא זה ששולט".

"נצטרך להתאים לכך את הרגולציה הישראלית, להגדיר מחדש מהו סוד מדינה ולהתאים את חוק השב"כ, שנכתב בעידן הסיגינט, לעידן הסייבר וה-AI", הוסיף. הוא הבטיח שהשב"כ ימשיך להיות אג'ילי בתחום הטכנולוגיה. כך, אמר, "נזדקק לשיתופי פעולה ופתיחות בין ענקיות הטק לגופי הביטחון".

לסיכום ציין בר כי "תפיסת הביטחון של ישראל מבוססת על שכבות ההרתעה, ההתראה, ההכרעה וההגנה. עלינו להוסיף שכבה נוספת – ההשפעה. הרשת מעניקה למדינות ולארגונים קרקע פורייה להסית, להשיג מידע רגיש, לקיים מגע ולפעול. אנחנו מזהים את המגמות האלה בשלבים מוקדמים, מצויים בנבכי הרשת ורואים היטב את המתרחש בה: ריגול, טרור, הסתה והשפעה זרה. בעולם המלחמה החדש, הניצחונות נספרים במספר השרתים שבהם יש למדינה דריסת רגל, ולא במספר הגבעות שעליהן מתנוסס דגל – ונדרש להגן על השרתים. על הסייבר יש להגן תשתיתית, ובשלושה רבדים: המקומי, עם כיפת ברזל מבוססת AI, שתאתר, תחקור ותבלום אנומליות שמגיעות לישראל; הבינלאומי, עם בריתות כמו אינטרפול בתחום הסייבר ואגם נתוני מודיעין איומים; וברובד ה-B2G, שמחבר בין ממשלות וחברות בתעשייה".

PC אנשים ומחשבים

ראש מערך הסייבר: ”מי שמבצע מתקפות נגד ישראל ישלם מחיר”

”איראן פועלת בסייבר לא רק נגד ישראל, אלא בכל המזרח התיכון”, אמר ראש מערך הסייבר הלאומי, גבי פורטנוי. הוא קרא לשיתוף פעולה בינלאומי נגד האיום הקיברנטי האיראני - ונגד הרעים האחרים

יוסי הטוני

”קבוצות האקרים מאיראן פועלות לא רק נגד ישראל, אלא תוקפות מטרות אזרחיות במדינות רבות, בהן טורקיה, ערב הסעודית, מצרים, מרוקו, הודו, בחריין, עומאן, כווית ועוד. בשנה האחרונה איראן ניסתה לתקוף גופים נוספים בישראל, לרוב ללא הצלחה. מי שמבצע מתקפות סייבר נגד ישראל צריך לקחת בחשבון את המחיר שהוא ישלם על כך”, אמר גבי פורטנוי, ראש מערך הסייבר הלאומי.

פורטנוי דיבר היום (ג׳) בשבוע הסייבר באוניברסיטת תל אביב. הוא ציין את קבוצת התקיפה MuddyWater, המשויכת למשרד המודיעין והביטחון של איראן, שתקפה את הטכניון לפני כמה חודשים. ”הקבוצה עובדת לא רק נגד ישראל, אלא תוקפת מטרות אזרחיות במדינות רבות במזרח התיכון”, אמר.

”קהילת הסייבר הישראלית מכירה את פעולות הסייבר של האיראנים מבפנים ומבחוץ, ועובדת לשבש אותה בדרכים שונות. אנשי משרד המודיעין האיראני, אנשים ממשמרות המהפכה והחיזבאללה שמעורבים במבצעי סייבר נגד ישראל יודעים בדיוק על מה אני מדבר”, ציין.

ואלה שמות

פורטנוי חיזק את ”פעילות ארצות הברית נגד האלימות האיראנית ואת הסנקציות שהיא השיתה על שני ׳שחקנים׳ ממשרד המודיעין האיראני – פרזין כרימי ומג׳תבא מצטפוי, שייסדו את אקדמיית ראווין. זו מאמנת האקרים למטרות

”קשה לפעול נגד פשע שבמהותו הוא חסר גבולות”

”קשה לגוף אכיפה בינלאומי לפעול נגד פשע, שבמהותו הוא חסר גבולות”, הסביר ג׳ונס. ”המנדט של האינטרפול מונע מאיתנו לעסוק בכל דבר – מלבד פשע שהוא פוליטי, ספרותי, גזעני או דתי. זה מגביל מאוד את היכולת שלנו לזהות, לנטר ולתפוס את המבצעים של פשעי סייבר – כי זה אומר משהו אחר בכל מקום. אנחנו מוגבלים על ידי החקיקות הפרטניות של מדינות. למשל, לפי חוק הגניבה של בריטניה, מ-1960, אדם אשם בגניבה אם לקח לבעלותו, לא ביושר ולצמיתות – רכוש השייך לאחר. אלא ש׳מידע׳ ו-׳נתונים׳ – לא כלולים תחת הגדרה זו”.

ג׳ונס תיאר את מקרה ”החותם השחור”, הראשון בו נתקל, ב-2014, במסגרתו נפרצה בסייבר ענקית הצעצועים האלקטרוניים הסינית, Vtech. ההאקר שאחראי לפריצה, השיג מידע אישי של כמעט חמישה מיליון הורים, לקוחות החברה, ושל יותר מ-200 אלף ילדיהם, כמו גם מאגר בהיקף של מאות ג׳יגה-בייטים – שכלל תמונות פרופיל, קבצי אודיו ויומני צ׳טים, שמרביתם שייכים לילדים.

”קיבלתי שיחת טלפון מעורך דין של החברה”, סיפר ג׳ונס. ”בדיוק הקמתי יחידת סייבר חדשה, כי אף אחד לא רצה לעשות את זה. לאחר שיחות רבות, הוא הודה בזהות הלקוחה. צחקתי: ׳1234 App me׳ אינה באמת סיסמה טובה להגנת המערכות. אדם בודד נכנס למערכות שלהם, היה המום ממה שמצא, חילץ את כל הנתונים האלה, הצפין אותם ואחסן בשני בסיסי נתונים, בקריביים ובגרמניה. כשתפסנו את ההאקר, צצה בעיה: הנתונים אינם רכוש לפי החוק הבריטי. אלא שניצלתי סוג של שטח אפור, כי פעלנו בגרמניה. זה היה אירוע החותם השחור הראשון ׳שלי׳. האירוע הבא היה WannaCry ב-2017: אז אנשי הבינו שהמודל שלנו לא מספיק טוב כדי להתמודד עם תקרית שכזו. לא ניהלנו בצורה יעילה את המאבק במסגרת המשאבים וההגדרות לפעילות שלנו”.

”בתוכנית למאבק בפשעי סייבר של האינטרפול”, ציין ג׳ונס, ”אנו פועלים למנוע פשעי סייבר, לחקור אותם ולהביא לשיבוש של פשעי הסייבר. אבל אנו עובדים מול מי שאינם הנפגעים ישירות מפשעי סייבר, אלא הצדדים השלישיים – חברות אבטחת מידע כמו טרנד מיקרו, קספרסקי, פורטינט ופאלו אלטו. רק באחרונה התחלנו לעבד נתונים במשותף איתן. כעת אנו מעניקים להן גם פלטפורמות מאובטחות לשיתופי מידע ותקשורת”.

”כשהתחלתי את דרכי ב-1990”, סיכם ג׳ונס, ”לא נדרשתי לטשטוש הקווים סביב שחקני האיום והפושעים – מי פועל ממניע כספי ומי שלוח מדינה. הייתי שוטר בטוטנהאם, שעסק בהרגעת הסדר באצטדיוני כדורגל שאכלסו 80,000 איש. הדבר הגרוע ביותר היה מכות. הפרדנו בין האוהדים של הקבוצות היריבות, היו מעט אפים מדממים, כמה מעצרים, והם שוחררו למחרת. אני מאמין שבעתיד יהיה לנו ברבור שחור – איזשהו צומת ש׳יחבר׳ בין הפגיעויות והמערכות של הרשתות, ולא משנה מי יהיה שחקן האיום. אם נוכל לחבר את הידע על הפגיעויות הללו במערכות וברשתות, אם נוכל להשתמש בטכנולוגיה – אז נוכל לחנך, נוכל להעלות את המודעות לתחום. לא נצליח לעצור את פשעי הסייבר, כיוון שלא עצרנו את הפשע בכל מקרה. אבל אכיפת החוק משתנה לאט, כשאנחנו מסתכלים על הגבולות הללו”.

זדוניות. כמו כן, עלי חידרי, שיושב בביירות, מתאם שיתוף פעולה בין איראן לחיזבאללה לשם גרימת נזק לאזרחי לבנון במרחב הסייבר״.

״עבור חלק מהאנשים במשרד המודיעין האיראני, להזיק לאזרחים מהשורה בעולם זה חלק מהשגרה״, ציין. פורטנוי קרא לקהילה הבינלאומית ״לעבוד יחד כדי לעצור אנשים כמו כרימי, מצטפוי וחידרי מפעילותם הזדונית נגד העולם״.

פרויקטים שמערך הסייבר מבצע

לדברי פורטנוי, ״מערך הסייבר פועל להעלאת החוסן וההגנה במשק, ועושה זאת עם כמה פרויקטים שהוא מקדם: כיפת הסייבר הישראלית, מרכז בקרה לאומי על בסיס טכנולוגיית ענן של גוגל, פורטל שירותי סייבר לארגונים ושירות PDNS לארגונים קריטיים. יש לנו פרויקט עם מיקרוסופט ואיחוד האמירויות לבניית פלטפורמה לשיתוף פעולה בחקירות סייבר ובניית ידע לשיתוף בין 40 מדינות. היוזמה היא חלק מפורום של הבית הלבן למאבק במתקפות כופרה. כמו כן, אנחנו עובדים עם מומחים בינלאומיים כדי לחקור מתקפות סייבר, ועם קהילת חוקרי הסייבר הישראלית כדי לגלות פגיעויות במערכות ממוחשבות ולטפל בהן״.

לסיכום הוא אמר כי ״פעילות הגנת הסייבר נדמית למסע בין כוכבים, במובן של הגנת האומה, תוך חיפוש וחשיפת ציביליזציות חדשות, שאותן אדם טרם ראה. להצלחת המאמץ נדרש אומץ, כדי לפרוץ גבולות ולהגיע למחוזות חדשים. יחד נעוף מהר וגבוה יותר. כדי שזה יתאפשר, נדרשים שיתופי פעולה בינלאומיים, שיתופי ידע ומודיעין איומים. על הטובים בעולם להיות מסונכרנים. רק באמצעות שיתופי פעולה תוך ישראליים ועולמיים נצליח לבנות את ‹כדור הבדולח› לחקירת אירועים ולהגנה מוכללת בסייבר. כולנו מתמודדים עם אתגרים דומים, וככל שנלמד ונדבר באותה השפה, כך ניטיב לשפר את ההגנה בסייבר. זו משימה שאינה נגמרת, זהו מסע אינסופי״.

ice.

אמור לי מי הם שותפיך ואומר לך כמה אתה מוגן

השותפים או קבלני המשנה של הארגון עשויים להיות הדבר שיגרום למתקפה מוצלחת עליו. ד״ר יניב הראל מסביר לרגל שבוע הסייבר מה ניתן לעשות

לאורך שנים נהוג לחשוב שבתחומים בהם ניתנת אחריות, בפרט בהיבטים טכנולוגיים ארגוניים, מידת ההערכות וטיב הפעולות הנעשות הן המפתח לרמת הביצועים והתוצאות המתקבלות. גם במקרה של הסייבר בחלק גדול מהדברים יש השפעה ישירה לבנייה והערכות שנעשות בשוטף על רמת ההגנה או על החוסן של הארגון שבונה את יכולותיו.

אם ארגון משקיע תקציב גדול, מאייש צוות חזק, בונה מתודולוגיית פעולה, ומקדיש תשומת לב ניהולית לעניין – יש בהחלט סיכוי גבוה יותר שיצליח לעמוד בסוגי מתקפות סייבר שונות וגם במידה ואחת המתקפות תפגע בו, הנזק שייגרם יהיה נמוך יותר. ארגונים וחברות בשנים האחרונות מעלים בהדרגה, מתוך הבנת האיומים והמוחשיות של מתקפות סייבר, את ההשקעה בתחום וכל צורת הטיפול מתקדמת משנה לשנה בקצב גבוה.

לצד שביעות הרצון מההשקעה הפנימית בארגונים ותרומתה להגנה, קיים גורם אחר שלאורך שנים לא היה מטופל, הוא איננו באחראיות ישירה של החברה ועם זאת הוא עשוי להיות הדבר שיגרום למתקפה מוצלחת עליה. הגורם הוא רמת ההגנה של השותפים או קבלני המשנה של החברה. חברת TARGET האמריקאית נפרצה בשנת 2013 לא בגלל תוקפים שנכנסו לרשת שלה אלא בזכות היכולת לתקוף קבלן משנה של הרשת וממנו להצליח להשיג את נתוני הכניסה שאיפשרו לתוקפים להיכנס לרשת. מערך ההגנה של החברה לא כשל באופן ישיר מול התוקפים, אלא חברה קטנה משמעותית אחרת שמספקת שירותים לחברת TARGET נפרצה וממנה התוקפים עברו לתאגיד הגדול.

ברור לגמרי שתוקפים יעדיפו להתעמת עם חברה קטנה שיכולות ההגנה שלה ממוצעות, תקציביה קטנים, וצוות האבטחה שלה איננו גדול מאד, לעומת הניסיון לאתגר את קבוצת האבטחה של תאגיד גדול ציבורי ועתיר משאבים.

<tech12>

הצצה נדירה לתוכנית ה-AI השאפתנית של השב"כ למלחמה בטרור

יכולות AI מתוחכמות הפכו לכלי עבודה יעיל בשירות הביטחון הכללי. כעת מתנסים ראשי הארגון ברתימת הדור החדש של ה-AI הגנרטיבית סטייל ChatGPT לשיפור יכולות הסיכול של השירות. כך זה עובד

טל שחף

הנה סיפור מצמרר, שלא היה ולא נברא אבל דומים לו מתרחשים מדי שבוע: אור ראשון מבליח מעל גגות כפר פלסטיני בצפון השומרון. הרחובות ריקים מאדם. צעיר חיוור יוצא מאחד הבתים, נושא תרמיל על גבו, מסתכל בעצבנות סביבו. דקה אחר כך נעצר לידו טנדר מרוט, אוסף אותו ויוצא את הכפר בדרכו לצומת תפוח.

עשר דקות לאחר מכן המחבל שוכב כפות לצד הכביש, פניו כבושים בקרקע. מסביבו אנשי מג"ב, חיילים וגם כמה אנשי שב"כ בלבוש אזרחי. התיק שלו נסרק ונמצאה בו כמות נכבדת של סכיני מטבח ארוכי להבים. נהג הטנדר נעצר גם הוא, כשניסה להימלט מהמקום. מסע רצח שהיה עלול להסתיים בכמה הרוגים יהודים נעצר עוד לפני שהתחיל.

הנתונים מראים שמאז תחילת השנה התרחשו כ-150 פיגועים משמעותיים - מטען, דריסה, דקירה וכ-120 פיגועי ירי. פחות זוכרים שבנוסף להם היו 375 סיכולים של כוונות לבצע פיגועים כאלה, מהם 300 מקרים של כוונה לבצע פיגועי ירי. מי שאחראי לסיכול הפיגועים הוא שירות הביטחון הכללי (שב"כ). אחד הכלים העיקריים שלו במאמץ הזה היא הבינה המלאכותית.

באחד השבועות האחרונים התקיימה בשב"כ ישיבת מטה שירות, מה שמקביל לישיבת מטכ"ל בצה"ל. נושא הדיון היה מפתיע משהו: בינה מלאכותית יוצרת (Generative AI). כן, התופעה שאנחנו מכירים בתור ChatGPT או בארד מעסיקה בימים אלו את ראשי השב"כ.

השאלה שהם שואלים היא האם אפשר לרתום GenAI בשמה המקוצר כדי לשפר את יכולות הסיכול של השירות? האם פריצת הדרך הטכנולוגית הזו עשוייה להפוך את השב"כ ליעיל יותר, מדוייק יותר, זריז יותר?

הגישה שמוביל ראש השב"כ רונן בר גורסת שהזירה הביטחונית הישראלית נדרשת להוביל את קפיצת המדרגה המשמעותית בתחום ה-GenAI ברמה הלאומית, בשיתוף עם ענקיות הטכנולוגיה העולמיות, בהיבטי רגולציה ובהיבטי שיתוף ידע ויכולות.

בראייתו של בר, נכון ששב"כ יהיה הגורם המוביל בתחום בקהילה ומול שותפיה הביטחוניים של ישראל בעולם. את הגישה שלו בעניין מהפיכת ה-AI הוא יציג בשבוע הבא במסגרת כנס "שבוע הסייבר" השנתי של המרכז למחקר סייבר באוניברסיטת תל-אביב.

בינה מלאכותית גנרטיבית בשירות השב"כ היא רעיון שצריך לגלגל קצת בראש. זה דבר אחד לשאול את ChatGPT על מלחינים אוסטריים בולטים ולקבל כמה שמות של אנשים לא אמיתיים. זה דבר אחר לגמרי לשאול אותו מי עומד לבצע פיגוע הבוקר ולקבל רשימה של מחבלים בדויים.

אלא שבינה מלאכותית יוצרת היא כלי רב עוצמה שעד כה ראינו רק את קצה קצהו של יכולתה. והיכולת הזו היא לצלול לתוך אוקיינוס של נתונים ולהוציא מתוכו תובנות שאדם לא מסוגל למצוא ואפילו AI מהסוגים המסורתיים לא תצליח.

האמירה ש"קו ההגנה חזק כמו החוליה הכי חלשה בו" נכון במקרה זה בצורה מובהקת.

לאורך השנים האחרונות חברות מזהות את חשיבות האיום של צד שלישי. כשלמעשה הכוונה איננה לאיום של צד שלישי אלא לסיכון שהחיבור וההתממשקות לצד שלישי מטיל על החברה. ארגונים נוהגים בימינו לערוך ניתוח של כל גורמי הצד השלישי שיש להם פעילות איתם. הפעילות מנותחת במישור של חשיבות הקשר, סוגי המידע שיש אליהם, נגישות, ורמת הקירבה של החיבור. לדוגמא, עשויה להיות חברה שהינה הספק המרכזי ביותר של ארגון מסויים, אין ספק בחשיבותו, אולם הוא מספק מרכיב שהיא פיזי במהותו וכל האינטראקציה עם הספק הוא קבלת הצעות מחיר והוצאת הזמנות אליו.

סוג חיבור כזה לא ידורג כמאוד בעייתי מבחינה סייברית כיוון שיחסית קל להגן עליו ואין בו סיכון גדול, למרות שכספק יתכן שהוא הספק החשוב ביותר של הארגון. מנגד עשוי להיות גורם אחר שיכול להיות החברה שמטפלת במתנות לחג או יועץ פנסיוני לעובדים או אחר שמסיבה מסויימת מחובר לרשת, מקבל נתונים על כל העובדים וגם מבצע פעולות מסויימות ולמרות שאולי חשיבותו העסקית נמוכה הוא עשוי להוות סיכון סייברי מהותי.

חברות וארגונים היום, מבצעים ניתוח של שותפיהם ומחליטים על צעדים שוטפים שאמורים לוודא ששותפים אלו מתנהלים בצורה סייברית מקצועית ואחראית ובמידת האפשר מצמצמים את החשיפה אליהם ואת רמת הקישוריות המוגדרת. שינויים אלו בתפיסות, בשיטות העבודה ובטכנולוגיות התומכות הם חלק מהנושאים שיידונו בשבוע הבא בשבוע הסייבר הלאומי המתקיים באוניברסיטת תל-אביב ואליו צפויים להגיע אלפי אנשים מישראל וממדינות אחרות להשמיע, להחליף דעות וללמוד.

הכותב הוא ראש תחום אסטרטגיה (CSO) במרכז למחקר סייבר באוניברסיטת ת"א, אשר יערך בין 26-29.6 את שבוע הסייבר השנתי באוניברסיטת ת"א בשיתוף מערך הסייבר הלאומי, משרד הכלכלה ומשרד החוץ

ואם אלה יהיו תובנות מצילות חיים, אולי כדאי לגלגל את הרעיון הלאה, בזהירות.

מאגר עצום של נתונים שמספק תובנות בזמן אמת

אוקיינוס של נתונים זה בדיוק מה שהשב"כ מחזיק ברשותו - מיליארדי נתונים שנאספים מדי יום. הנתונים האלו נצברים בדרכים שרק הדימיון יכול לשער: הקלטות של שיחות טלפון ושיחות בעל פה, צילומים וסרטוני וידאו, מידע מכל הסוגים שעובר ברשתות החברתיות ובאמצעות רשתות אחרות.

הדיווחים מגיעים מחיישנים בשטח, ממצלמות קבועות וניידות, ממעקבים, מהאזנות, מדיווחים של משתפי פעולה. כל הנתונים האלה מגיעים למאגרי השב"כ העצומים, ועוברים תהליכי פענוח וניתוח שנועדו להפוך אותם לחומר גלם למערכות המידע ולבינה המלאכותית.

למחבל מתחילת הכתבה היה מראש סיכוי קטן להצליח. מערכות הביג-דאטה העצומות של השב"כ יודעות הכל על כולם. גם אם הוא ינסה להסתיר את מטרותיו - והפלסטינים הרי יודעים שהם תחת מעקב מתמיד - רוב הסיכויים שהוא ייחשף.

המערכת יודעת עליו הכל: לאן הוא הלך, מי החברים שלו, מי המשפחה שלו, מה מעסיק אותו, מה אמר ומה פרסם. באמצעות הבינה המלאכותית המערכת מנתחת התנהגות, מנבאת סיכונים, מקפיצה התרעות ומסבה את תשומת הלב של אנשי "הפאודה" למי שכדאי לשם אליו לב.

מערכות AI אחרות מסייעות לדובב נחקרים בחדרי חקירות. מול החוקרים יש מסך נתונים, וכל אמירה של הנחקר מאומתת ומוצלבת בזמן אמיתי. אם הוא משקר – המערכת תדע לציין את זה. הלם המידע הזה על הנחקר מאפשר לדובב אותו לפני שהוא "מתקרר" בשפת השב"כ. מספיק לתכנן מה להגיד ואיזו גירסה לבנות.

תחקיר של ידיעות אחרונות חשף לפני כמה שנים את "הכלי": מאגר המידע הסודי של השב"כ שאוסף נתונים על כולם, גם על אזרחי מדינת ישראל. זה הכלי שגויס למאבק בקורונה. בראיון ב-2020 חשף ראש אגף טכנולוגיות המידע הקודם של השב"כ ששי אליה את היכולות העצומות שיש למערכת הזו, שרוב הזמן ממוקדת בתושבי השטחים.

אבל לא רק פלסטינים נמצאים תחת מעקב. יש מערכות שמיועדות לאתר טרור יהודי בשטחים. בימים אלו גויסה המערכת שוב מול אזרחים ישראלים, הפעם כדי לזהות מקרים של אלימות בחברה הערבית שנמצאים על התפר בין פלילי לטרוריסטי. בתנאים מסוימים הממשלה עלולה להרחיב את היכולות האלה לכלל החברה הישראלית.

מאז הריאיון ההוא שהעניק אליה חלפו שלוש שנים, והטכנולוגיה הנוכחית של השב"כ העצימה את יכולותיה באופן אקספוננציאלי. האח הגדול של ג׳ורג׳ אורוול מחוויר מקנאה.

כתבה זו נסמכת על שיחות רקע ושיתוף פעולה עם גורמים בכירים בשב"כ, אלו שאמונים על התחומים הטכנולוגיים של הארגון. פעילות זו מתרחשת באגף טכנולוגיית המידע של השב"כ. מחלקה אחת באגף מפעילה מודלים של AI ואנליסטים, ושולחת אותם לחבור לחפ"קים קדמיים של השב"כ, לצד אנשי המבצעים. במקום אחר פועלת "סדנת ה-AI" של השב"כ - ככל הנראה אחד הגופים המתקדמים בישראל בפיתוח יכולות בינה מלאכותית.

לו זה היה תלוי באנשי הטכנולוגיה של השב"כ, עיקר הדיווח היה עוסק בנפלאות הבינה המלאכותית ובתרומתה להפיכת הארגון לכזה שמונע על ידי נתונים. יש כאן הרבה דברים מלהיבים מבחינה טכנולוגית, אבל במקרה זה מטרות הטכנולוגיה מחייבות כובד ראש מסוג אחר. אחרי הכל מדובר ברתימת הטכנולוגיה למעצרם ואפילו לחיסולם של אנשים. מצד שני, היא גם מסייעת להצלת חייהם של הרבה אנשים אחרים. נושא מעיק, לגיקים יהיה קשה כאן.

ובכל זאת, שב"כ מעסיק את מיטב אנשי המקצוע, מומחי AI ומדעני נתונים. לא מן הנמנע שהמוטיבציה של הארגון להיחשף כאן נועדה בין השאר למשוך אנשים נוספים להצטרף לשירות.

לסדנת ה-AI של הארגון שהוקמה לפני כשלוש שנים גויסו מומחים מהאקדמיה ומהתעשיה: יזמי הייטק שסגרו את החברה ועברו לשב"כ, כמה בעלי תואר דוקטור במדעי המחשב. מדובר בחבורה יוצאת דופן של אנשים מבריקים, שנהנים ממה שנחשב לגיזת הזהב של עולם הבינה המלאכותית: כמויות עצומות של נתונים והכלים הכי חזקים לפצח אותם.

המשימות שלהם משתנות מיום ליום ומשבוע לשבוע והן מרתקות: הבנת טקסט, ניתוח שמע, איתור התנהגות ויזואלית, בניית מודלי LLM. אפשר להניח שהאנשים בסדנה מונעים גם משכנוע עמוק בצדקת הדרך, בכך שהמערכות שהם מפתחים מצילות חיים, ואם אנשים מתים בגללן - אלה האנשים הרעים. אבל בסוף הטכנולוגיה הזו יש אנשים מתים, וזה אולי לא מתאים לכל הייטקיסט ממוצע.

יכולות הניתוח של ה-AI שולבו בשלל רמות הארגון

האתגר הטכנולוגי בשב"כ נובע מהצורך לקבל את התובנות מהר מאוד, כדי לאפשר סיכול מבעוד מועד. המידע הזה צריך להיות מוגש כך שיתמוך בקבלת ההחלטות של האדם המקבל: מפקד, אנליסט, דסקאי איש שטח. והוא צריך להגיע במשבצת זמן מאוד מצומצמת, לפני שהחשוד יספיק להבחין בהתרחשות ולהימלט.

"בהתמודדות עם עולם הביג-דאטה לא מדובר רק בבניית התשתית אלא גם בפיתוח מערכות וכלים שמנגישים את הדאטה – למי שצריך ואיך שצריך ולאיפה שצריך ומתי שצריך", אומר גורם בכיר בשב"כ.

"זה אומר לתת את פיסת המידע שדרושה לרכז שנמצא כרגע בשטח - אבל רק את המידע הספציפי על הבית שמעניין אותו. זו הדרמה הגדולה שמתרחשת כאן, של פיתוח מערכות וכלים עבור המשתמשים".

הפעילות הזו מבוצעת באמצעות מודלים של AI: מערכות בינה מלאכותית שאומנו לזהות מצבים ספציפיים, סימנים ספציפיים וקבוצת יעד ספציפית. כשעולה צורך מבצעי, במחלקה הרלוונטית מושיבים את מומחי ה-AI לייצר את המודל. בתוך ימים ספורים, לעיתים בתוך שעות, הם מפתחים את כלי ה-AI שמסוגל לספק מענה מדויק ולהציג איומים חמים ומיידיים. עד כה פותחו קרוב ל-80 מודלים כאלה, שמכונים מְבצעי נתונים: data operations.

במקביל פועלות מערכות AI אחרות - מערכות גדולות שפועלות באופן מתמשך ויודעות להציף איומים לרוחב השטח ולאורך הזמן. אלה מערכות כלליות, חזקות ביכולותיהן, ככל הנראה מהמתקדמות שמופעלות כיום בארגוני מודיעין ואכיפה בעולם.

וזה לא הכל. הבינה המלאכותית מסייעת גם בייעול העבודה הפנימית בשב"כ, כמו בכל ארגון ששואף להתייעל. קחו למשל תחום כמו תרגום: לאורך שנים פועלים בגופי המודיעין מאזינים, שצריכים לתרגם שיחות שהם קולטים מערבית לעברית. הכמות כל כך גדולה שהמאזין צריך לנסות ולזהות שיחה בעלת חשיבות לפני שהוא מתרגם אותה.

עכשיו זה משתנה. הבינה המלאכותית יכולה לתרגם בקלות את כל השיחות ובדרגת אמינות גבוהה יחסית. לאחר מכן ה-AI תסרוק את התכנים ותציף שיחות שיש בהן מידע מודיעיני. זו התייעלות משמעותית לא רק בדרך העבודה, גם ביכולת המבצעית.

והנה עוד משימה שהוטלה על הבינה המלאכותית של השב"כ: לבחון את שלל האיומים שנמצאים בכל רגע במערכת, ולהציג אותם לפי מידת הסיכון או המיידיות שנדרשת בטיפול בהם. כאן כבר מוטלת אחריות אמיתית על הבינה המלאכותית. היא יודעת לזהות את המקרים שאימנו אותה לזהות והיא עלולה להחמיץ מקרים שטרם הכירה. אבל הטכנולוגיה מתפתחת בקצב מסחרר והיכולות של ה-AI הולכות ומשתפרות.

"אנחנו יכולים לייצר מיקוד ותעדוף של טיפול באמצעות אלגוריתמים של AI שיודעים לזהות דפוסים ואנומליות. דברים שמאפשרים לנו להקדים, למנוע ולסכל", מסביר הגורם הבכיר. "זה מאפשר גם לתעדף את המשימות כי אי אפשר להתמודד עם כל הדברים ביחד.

"אם פעם היינו צריכים להתמודד רק עם טרור מאורגן ומכוון, היום זה גם טרור בודדים, גם טרור בסייבר, גם בתווך הקינטי, גם השפעה על תודעה. אלה דברים שהמכונה יודעת לעשות יותר טוב מאיתנו ואנחנו רוצים להיעזר בה".

השלב הבא של ה-AI: לחזות מראש אירועים

המשימה המאתגרת עוד יותר של הבינה המלאכותית היא לחזות אירועים והתרחשויות. היכולת הזו, שמבוססת למידת מכונה (ML), מוכרת היטב בעולם האזרחי: על סמך התנהגות של מיליוני מקרים וצירופי מקרים קודמים אפשר בוודאות גבוהה מאוד לחזות מה עומדים אדם מסויים או קבוצה מסוימת לעשות.

הבינה המלאכותית מצטיינת בזיהוי תבניות, כאלו שבני האדם פועלים סטטיסטית לפיהן בלי שהם אפילו מודעים לכך. כמות הנתונים העצומה שקיימת במערכות השב"כ היא בסיס מצוין לזיהוי תבניות של התנהגות שעלולה להוביל לפעילות טרור. מבצעי טרור יחידים עשויים לעלות כל הכוונת עוד לפני שהם קיבלו את ההחלטה לצאת לפיגוע.

עכשיו מגיע השלב הבא, שנראה עדיין קצת מדע בדיוני: הכנסה לשימוש של בינה מלאכותית גנרטיבית, הטרנד הכי חם בעולמות הטכנולוגיה כיום.

"במקום שבו יש את האתגר שיש לנו, אין לנו ברירה אחרת אלא לחבר את הבינה המלאכותית בכל הרבדים", מפרט הגורם הבכיר. "זה למידת מכונה, זו למידה עמוקה, זו בינה מלאכותית צרה שמיוצרת למשימות מאוד ספציפיות. וזה מגיע עד להתפתחויות האחרונות של בינה מלאכותית יוצרת (GenAI) ובינה מלאכותית כוללת (AGI). לשם אנחנו הולכים".

בחודשים האחרונים התחילו באגף הטכנולוגיות לפתח כלים ראשונים בטכנולוגיית GenAI. הם לא מסתפקים בלשאול את הצ›טבוט על דברים שקורים בעולם החיצוני, אלא מפעילים את הטכנולוגיה על הנתונים של השב"כ עצמו, במערכת שפועלת על מחשבי ה-AI העצומים של הארגון. מדובר בצעדים ראשונים, אבל הפוטנציאל נראה עצום, וגם מפחיד.

בינה מלאכותית גנרטיבית יודעת למצוא תובנות בכוחות עצמה, בלי שלימדו אותה, והתוצאות עלולות להיות לא מוסברות. רשימת חשודים בכפר מסוים עלולה לכלול שמות של אנשים שבשום כלי אחר אי אפשר היה לעלות עליהם - אבל חלק מהשמות האלה עלולים להיות טעות.

אנשי הטכנולוגיה של הארגון מדברים על מערכת GenAI שתעמוד לרשות מקבלי ההחלטות בשב"כ, כזו שתוכל להמליץ על דרכי פעולה בצורה אובייקטיבית שמנטרלת אגו ורעשים. זה כמו ChatGPT של קבלת החלטות אסטרטגיות.

עכשיו גם מתחילות מחשבות ראשונות על השלב הבא של הבינה המלאכותית: הבינה המלאכותית הכוללת (AGI). העולם כולו אחוז בחרדות לקראת האירוע הזה, שהוא כנראה בלתי נמנע.

ה-AGI לא תחכה להנחיות של מפעילים אנושיים. היא עשוייה למצוא ליקויים בתורת ההפעלה של השב"כ ולהציע דרכי פעולה שאיש לא חשב עליהן, ושיביאו לתוצאות שאיש לא ציפה להן.

אחת המחשבות היא שה-AGI תפתח תודעה משל עצמה, והשילוב בין דעתה על המצב בשטחים לבין יכולות הפעולה מרחיקות הלכת של השב"כ צריכות להדאיג את כולנו.

ה-AI תלמד מה הסוכנים רוצים ותהיה ממוקדת יותר

המהפך הגדול שעבר השב"כ לארגון שמונע על ידי נתונים לא התחיל עכשיו. מאז תחילת שנות ה-2000 החלו בארגון לאסוף נתונים ולצבור אותם במערכות מידע. הניתוח שלהם אז היה ידני בעיקרו, בעזרת מערכות תמיכה בהחלטות (BI).

אבל היקף המידע הלך וגדל, והכלים לניתוחו הלכו והשתפרו. בתקופתו של ראש השב"כ הקודם, נדב ארגמן, הוחלט על איחוד גורמי הטכנולוגיה, הסייבר והסיגינט (האזנות) ליחידה אחת: אגף טכנולוגיות המידע.

"ברקע היתה מהפכת התפוצצות המידע, שזו הדרמה הגדולה שמלווה אותנו בעיקר בעשר השנים האחרונות", מפרט הגורם הבכיר בשב"כ. "השירות נדרש לאסוף הרבה מאוד מידע, למצות אותו, לסנן אותו ולזקק אותו לתובנות מודיעיניות, וזה האירוע הדרמטי כאן.

"היינו צריכים להכין את השירות למהפיכה, החל מרמת תשתיות המחשוב שיקלטו את כל הנתונים ויעבדו אותם, ועד ליצירת תפקיד מנהל הדאטה ראשי (CDO), שאחראי לגבש את אסטרטגיית הדאטה הארגונית. זאת מיומנות מאוד גדולה לתת מכל ים הדאטה שקיים את מה שבאמת נדרש ואיפה שהוא נדרש".

לפי התיאור שלו, השב"כ הוא ארגון שהשלים את תהליך הטרנספורמציה שרבים בעולמות העסקיים עדיין מדברים עליו. הארגון לא רק הכיר בטכנולוגיה החדשה ומיישם אותה בכל תחומי הפעילות - הוא גם הפך אותה למנוע לשינוי הארגון כולו. העובדים בכל רמות הארגון משתמשים בכלי AI כאלה או אחרים. ובפעילותם המבצעית הם גם תורמים לפיתוח ושיפור הכלים שמפעיל השב"כ.

מכירים את זה שביוטיוב או בטיקטוק התגובות שלכם לתוכן משנות את הדרך שבה אלגוריתם הצעות התוכן מתאים את התכנים לטעמכם? דבר דומה קורה במערכות ה-AI של השב"כ, אם כי למטרות שונות בתכלית.

כלי ה-AI לא מסתפקים בהצגת התרעות, הם גם עוקבים אחרי השימוש של העובדים במידע.

בחלק מהמקרים העובדים גם נדרשים לתת פידבק קונקרטי. התוצאה היא שההתרעות הבאות של המערכת יהיו הרבה יותר ממוקדות ויובילו לסיכולים יותר מובהקים. ובינתיים דרך העבודה של הארגון עוברת שינויים בעידן הטכנולוגיה.

חייבים להתייחס גם לסיכונים בשימוש ב-AI. ככל שהיא נעשית מתוחכמת יותר, וככל שהיא עוברת ללמידה עצמאית ולא מפוקחת, כך התוצאות שהיא מניבה עלולות להיות פחות מובנות לבני האדם. זו אחת הבעיות המרכזיות בעולמות ה-AI הגנרטיבית הנוכחיים.

בשב"כ מדברים על בינה מלאכותית אחראית ועל בינה מלאכותית מוסברת, ועומלים קשה כנגד מה שמוצג כסכנה הכי גדולה: שהבינה המלאכותית תרד מהפסים. אם זה קורה לחברת ביטוח, היא עלולה להפסיד לקוחות. אם זה קורה לשב"כ, כמה אנשים חפים מפשע עלולים להיות בסכנה גדולה.

"יש איזורים שבהם אתה צריך לתפור את המגבלות כדי שהמודלים לא יטעו אותך", מנסה הגורם הבכיר להרגיע. "אתה צריך לבדוק את עצמך, לוודא שהמודלים לא יורדים מהפסים. שהשימוש בהם הוא שימוש אחראי. אנחנו תמיד נתייחס ל-AI כאל עוזר. בסוף תמיד נצטרך להיות ביקורתיים. החינוך שלנו הוא להטיל ספק וגם ב-AI אנחנו נטיל ספק".

<tech12>

קרן YL ונצ׳רס: "התחום המוביל בסייבר - אבטחת AI"

יואב לייטרסדורף, שותף-מנהל בקרן: "כ-70% מצוותי הסייבר שנפגשנו איתם בחודשים האחרונים עסקו בבניית מוצר בתחום". השקעות הסייבר בשוק הישראלי מתחילת השנה: 631 מיליון דולר

אמיתי זיו

יזמים ישראלים זזים מהר, וכעת מסתבר שרבים מהם כבר זיהו את האיומים הנלווים למהפכת ה-AI שאנו חיים אותה בימים אלו. "התחום המוביל כיום בקרב יזמי סייבר, בפער, הוא תחום ה-Security for AI. כ-70% מצוותי הסייבר שנפגשנו איתם בחודשים האחרונים עסקו בבניית מוצר בתחום", אומר יואב לייטרסדורף, שותף-מנהל בקרן הסייבר YL ונצ‹רס.

הדברים עולים מדוח מסכם של YL שעוסק בחציון הראשון של 2023. "השימוש הגובר בכלי בינה מלאכותית גנרטיבית (Generative AI) חושף ארגונים לסיכונים חדשים ומתוחכמים יותר, שכן תוקפים ישכילו לנצל את הפערים במוצרי סקיוריטי קיימים שאינם ערוכים לטפל באיום החדש", נכתב.

מוצרי סקיוריטי עבור AI יידרשו להגן על ארגונים לא רק מפני גניבת דאטה, לדוגמה, אלא גם מפני מניפולציה של הדאטה, שתילת דאטה מוטעה (‹הרעלת דאטה›) ומגוון היבטי פרטיות ושימוש לרעה בדאטה ארגוני. בנוסף, תקיפות ‹קלאסיות› כמו ‹פישינג› או הנדסה חברתית יהפכו למורכבות ומאיימות הרבה יותר על ידי שימוש ב-AI".

בקרן צופים שבעתיד הקרוב תחול גם רגולציה שתדרוש מארגונים לעמוד בסטנדרט אבטחה לשימוש ב-AI, דבר שיגביר את הביקוש למוצרים מהסוג הזה. "לא מעט שחקנים בתעשייה מעריכים שאנו בפתחה של מהפכה טכנולוגית בתחום ה-AI בדומה לזו שהייתה עם המעבר לענן", נכתב במחקר, "ואנו צופים שהפוטנציאל הקיים לחדשנות באבטחת טכנולוגיה זו רק ילך ויצמח". מדובר לא רק במוצר אחד, טוענים בקרן, אלא בעולם שלם של מוצרי הגנה חדשים, כפי שקרה במהפכת הענן.

תחומי השקעה בולטים נוספים שמזהים מומחי YL בחציון החולף הם Identity and Access Management - תחום שמשך כ-30% מההשקעות לאורך השנה. "כמות הזהויות בארגונים הולכת וגדלה לאור המשך המגמות של עבודה מרחוק, שימוש במוצרי SaaS, סביבות מחשוב מורכבות בענן ועוד. חלק משמעותי מהזהויות הללו הוא דווקא Machine Identities - מכונות, שרתים ושירותים המתקשרים אחד לשני", נכתב. תחומים "חמים" נוספים שזיהתה הקרן בהייטק הישראלי הם אבטחת ענן, ניהול חולשות וסיכונים, אך ירידה בתחומים חמים מהעבר הקרוב כמו Zero Trust ואבטחת מוצרי SaaS - "בהם לא היו השקעות חדשות השנה".

"מענה למספר רחב של צרכים"

עוד במסגרת הדוח, YL ונצ‹רס ערכה סקר בקרב יועציה וסמנכ"לי אבטחת מידע בחברות גלובליות. מהסקר עולה כי המשבר נותן את אותותיו והאחראים על תקציבי אבטחת המידע מחפשים התייעלות. כך נכתב: "שאלנו עשרות סמנכ"לי אבטחת מידע על השפעת המציאות הכלכלית על ההוצאות התקציביות וסדרי העדיפויות שלהם ברכישת מוצרי סקיוריטי. על אף חוסר היציבות הכלכלי המתמשך, נראה שתקציבי הסקיוריטי בארגונים לא נפגעו - בעיקר לאור התגברות האיומים והמשך תקיפות סייבר. יחד עם זאת, בעוד שבשנים האחרונות סמנכ"לי אבטחת מידע שמו דגש על חדשנות וחיפשו טכנולוגיה פורצת דרך, מהסקר החדש עולה כי כיום, ולאור המצב בשוק, הדגש הוא על התייעלות. סמנכ"לי אבטחת מידע כיום לא מעוניינים בהגדלת מספר מוצרי הסקיוריטי בארגון, אלא בוחרים באופן מושכל בפלטפורמות שמעניקות מענה רחב למספר צרכים, בין היתר בשל היעדר כוח אדם להתמחות ותפעול של מספר מוצרים במקביל".

תופעה זו יכולה להסביר למשל את החוזקה שהציגה פאלו אלטו נטוורקס בדוח האחרון מול החולשה היחסית בחברה כמו סנטינל וואן. הלקוחות מעדיפים להרחיב את המוצרים בפלטפורמה הקיימת, ופחות נלהבים להכניס לארגון סטארט אפים או כלים חדשים באופן כללי.

"להימכר ולא להיסגר"

ב-YL ונצ‹רס אף סיכמו את ההשקעות בתחום הסייבר בשוק הישראלי. סך הכל נרשמו בשוק 18 השקעות עד כה ב-2023 בסכום מצרפי של 631 מיליון דולר בחברות סייבר. זאת אומרת, בהכפלה פשוטה, קצב של 36 השקעות בשנה (מול 94 בשנת 2022) וסכום מצרפי חזוי של כ-1.2-1.3 מיליארד דולר בהשקעות מול 3.2 מיליארד דולר שזרמו לסייבר ב-2022. האטה משמעותית המאפיינת את כלל השוק. הנתונים יוצגו ויורחבו על ידי הקרן במסגרת שבוע הסייבר השנתי אשר ייערך בשבוע הבא באוניברסיטת ת"א.

לאורך החציון, עיקר הסבבים היו בסיד, כאמור 18 במספר, מול 5 סבבים בלבד בשלב A; שני סבבים בשלב B ו-4 סבבים בשלב C. באשר לאקזיטים - יש דווקא מגמה חזקה עם 9 אקזיטים לאורך הרבעון, מול 14 ב-2022 כולה, אבל רוב האקזיטים האלו קטנים, וחלקם גם ניצול הזדמנות מצד הרוכשת לקנות חברה במחיר זול.

ניתן לציין את האקזיטים הקטנים יחסית של פולאר סקיוריטי, מינרבה לאבס, קנוניק, ניאו-סק, Enso ו-Indeni. מבין האקזיטים הגדולים ניתן למנות את סיידר שנמכרה לפאלו אלטו נטוורקס ב-200 מיליון דולר; את הרכישה של אקסיס סקיוריטי על ידי HP ב-500 מיליון דולר ואת הרכישה של לייטספין על ידי סיסקו ב-250 מיליון דולר. מגמת האקזיטים הקטנים תימשך, מעריכים כותבי המחקר: "חברות רבות, בעיקר בשלבים יחסית מוקדמים, יעדיפו להימכר על מנת שלא להיסגר".

"בניתוח של שש החודשים הראשונים של 2023, ניתן לומר בבירור כי תעשיית הסייבר הישראלית לא חזרה לימי הזוהר של 2021 והמגמה הזו ככל הנראה תימשך בשנה הנוכחית", מסכמים בקרן. "ראינו בחציון הראשון של שנה זו המשך התפכחות של יזמים ומשקיעים כאחד, האטה עד כדי עצירה של גיוס סבבים מתקדמים ועלייה משמעותית בעסקאות רכישה - לצד המשך השקעות בשלבי סיד".

עוד הוסבר על הסיד: "השקעות בחברות צעירות פחות נפגעו מהמצב הנוכחי שכן איומי הסייבר רק גוברים ועדיין קיימות הזדמנויות רבות לחדשנות ויזמות בתחום. בנוסף, חברות שמגייסות סיד בתקופה הנוכחית ייתכן שיגיעו לסבבים הבאים אחרי חלוף המשבר".

ובכל זאת, יש ירידה במספר העסקאות, גם בסיד. "זה נובע משינוי גישה", מוסבר, "כי יזמים מעדיפים ואף נדרשים להגיע למשקיע פוטנציאלי עם רעיון מהודק, מבוסס ומבטיח, לאחר תהליך בחינה ארוך יחסית, זאת בניגוד לתהליכי ההשקעה המהירים של שנת 2021, שאז ניתן היה לראות סבבי גיוס בצוותים ללא רעיון מגובש". בסבבי A, נכתב, המשקיעים כבר רוצים לראות לקוחות משלמים והכנסות בפועל. והשקעות בחברות צמיחה כמעט לא קרו, בגלל סוגיית השווי - תופעה שמוכרת מכלל השוק.

<tech12>

מי התחדש בטייטל המגניב Head of Gaming ומה קורה בקבוצת Travelier?

ישנה בדיחה ישנה על כך שאנשים שעוסקים בסייבר אוהבים להגיד שהם עוסקים בסייבר, ואנשים שלא עוסקים בסייבר אוהבים להגיד שהם עוסקים בסייבר. את כל אלה כנראה תוכלו לפגוש בשבוע הסייבר הישראלי, שיתקיים מ-26 ועד 29 ביוני באוניברסיטת תל אביב. בין הדוברים בכנס תוכלו למצוא בכירים ישראלים ואמריקאים, מראש השב"כ ועד ראשת משרד הסייבר של הבית הלבן. לכנס צפויים להגיע כעשרת אלפים משתתפים.

ישראל היום
הכי ישראלי כל הזמן

ראש השב"כ רונן בר: "מזהים את הזרוע הארוכה של איראן מאחורי התארגנויות טרור שסיכלנו"

עוד אמר הבכיר הביטחוני במהלך כנס שבוע הסייבר: "הבינה המלאכותית תעשה מהפכה גם בעולמות המודיעין" • הוא הוסיף: "ארגוני הביטחון המסורתיים נדרשים להתאים את עצמם למצב החדש" • בכנס, המתקיים על רקע הדאגה הגוברת מפני מתקפת סייבר נרחבת העלולה לפגוע בתשתיות החיוניות בישראל, נאמו גם ראש מערך הסייבר הלאומי ומקבילו האמירתי

דניאלה גינזבורג

ישראל זיהתה את איראן כעומדת מאחורי התארגנויות טרור שסוכלו לאחרונה על ידי השב"כ, כך אמר הבוקר (שלישי) ראש השב"כ רונן בר, בזמן נאומו בכנס שבוע הסייבר, שמתקיים באוניברסיטת תל אביב.

"אני מניח שרבים ידברו על הפוטנציאל שיש לבינה מלאכותית, ואני לא רוצה להרוס, אבל בתור נציג של גורם מודיעיני – אדבר על הסכנות שיש בטכנולוגיה", אמר בר בפתח דבריו בכנס, שמתקיים באוניברסיטת תל אביב.

"הרשתות החברתיות נמצאות איתנו כבר כעשור, והאתגרים בהתמודדות עם הסכנות מהן רק הולכים וגדלים. מאחר ומידע הוא כוח והוא עבר מהספריות למרחב המקוון, אפשר להגיד כי הרשתות החברתיות הפכו למקור הידע הכי רלוונטי לנו".

"הסכנות שאנו מזהים מהרשתות החברתיות היא אלימות, שלא נגמרת רק במילה הכתובה, היא עוברת להסתה שמובילה לאלימות, אותה האלימות והטרור שאנחנו מזהים ומסכלים בג<נין, שכם ובכל רחבי הרשות הפלשתינית. מאחורי ההתארגנויות הטרוריסטיות האחרונות שסיכלנו זיהינו את הזרוע הארוכה של איראן", הוסיף.

עוד אמר בר: "ההסתה שיש כיום לא מגיעה מהמסגדים, אלא מהטלפונים הניידים. מתקפת הטרור שהתרחשה בשנה שעברה בבאר שבע היא דוגמה מובהקת לכך. איש לא ידע שהטרוריסט הולך לתקוף – לא אשתו, לא משפחתו. רק העדות שעל המחשב שלו, שכללה תכנים קיצוניים של דאעש".

"ארגוני הביטחון המסורתיים נדרשים להתאים את עצמם למצב החדש, שבו כל אדם זועם עם גישה לאינטרנט עשוי להפוך למפגע בהחלטה של רגע".

"קצב האירועים כל כך גבוה, שכאשר הוזמנתי לכאן לפני כחודש, תכננתי לדבר בעיקר על ההשפעות של הרשתות החברתיות על הביטחון הלאומי, אך בעקבות אירועים שאירעו לאחרונה, הבנתי שה- Generative AI כבר כאן", אמר. "הרשת האיצה תופעות של חוסר משילות, יצירת ניכור בין אזרחים למוסדות המדינה והדרת בודדים ומיעוטים. מידע הוא כוח. מהספריות, האוניברסיטאות, הסמכויות הדתיות וזקני השבט, הכוח נדד לרשת, והרשת החברתית הפכה לשר החוץ שלו. לתופעות שצומחות ברשת יש השלכות חברתיות, שאינן קשורות באופן ישיר לביטחון הלאומי – האלימות לא מסתיימת במילים. אנחנו פוגשים את האלימות הגואה בקסבה, בצירים ובערים שלנו".

"גוב האריות הוא דוגמה לארגון טרור מסוג חדש, טרור דור ה-Z. ניתן ללמוד ממנו על האופן שבו מדינות וארגוני טרור מנצלים את הדור הצעיר. הארגון אינו אידיאולוגי, קם ומגייס ברשת, ומקבל את התמיכה שלו מהציבור בצורה של לייקים".

ישראל היום

ראש אגף התקשוב וההגנה בסייבר: "תוך שנים ספורות, כל הלוחמה תתבסס על AI"

את הדברים אמר האלוף ערן ניב במסגרת ביקורו בכנס "שבוע הסייבר" בתל אביב • מבקר המדינה, שגם נשא דברים בכנס: "אנחנו נבדוק כיצד והאם בינה מלאכותית מוטמעת בתוך מערכות המדינה ולא מנוצלת לרעה"

דניאלה גינזבורג

מבקר המדינה אנגלמן, ביקר היום (רביעי) בכנס "שבוע הסייבר 2023" באוניברסיטת תל אביב והתייחס לנושא הבינה מלאכותית (AI), תחום שמאוד מעסיק את מדינות העולם ואת מגזרי הטכנולוגיה וההיי-טק בתקופה האחרונה. "לצד היתרונות הרבים של הבינה המלאכותית, היא טומנת בחובה גם סכנות להתעצמות ארגוני טרור ופשיעה. על מבקרי המדינות לבדוק שמדינות המערב, וישראל בתוכן, מוכנות לעידן ה- AI", טען אנגלמן.

בדבריו חשף המבקר, המכהן גם כסגן נשיא ארגון המבקרים האירופאי (EUROSAI), כי משרדו יתחיל בביקורת על מוכנות המדינה לעידן הבינה המלאכותית (AI), אשר תיעשה בשיתוף פעולה עם גורמים נוספים באירופה כדוגמת מבקר האיחוד האירופי ומבקרי המדינות של בריטניה, גרמניה ומדינות רבות נוספות.

אנגלמן טען כי "הביקורת תתמקד בשלושה היבטים בנוגע לפעולות הממשלה ולהיערכותה: התמודדות עם סיכוני הבינה המלאכותית בהיבט הטכנולוגי, קידום רגולציה וחקיקה ויישום כלי בינה מלאכותית במערכות ציבוריות-מדינתיות".

לדבריו, "הבינה המלאכותית עשויה להביא לכדי התקדמות טכנולוגית רחבת היקף בתחומים רבים אך לצדה קיימים סיכונים רבים ובהם "פייק ניוז", שימוש ב-AI ע"י גורמי טרור ופשיעה וההיערכות לשינויים הדרמטיים בשוק העבודה".

הוא הוסיף כי "בנושא הטכנולוגי נבדוק האם הממשלה מוכנה לטכנולוגיה החדשנית בהיבטי הממשל, יכולות המחשוב, ההון אנושי ועוד; בסוגיית הרגולציה והחקיקה נבדוק כיצד מגינה הממשלה על אזרחיה ועל עצמה על ידי הגבלת השימוש בטכנולוגיית AI שעלולה לגרום להשפעות שליליות ולחשוף את הציבור לסכנות. ההיבט השלישי הוא יישום בינה מלאכותית במערכות ציבוריות-מדינתיות. במסגרתו נבדוק האם וכיצד בינה מלאכותית מוטמעת בתוך מערכות

"מאחורי הקבוצה הזאת עומדת הזרוע הארוכה של איראן. היא מסמנת ברשת נוער מועד לפורענות, מסיתה, מעבירה להם כספים ומספקת להם ידע ונשק. ככה פשוט. גוב האריות, שחוסל בפשיטה של לוחמינו בקסבה, נולד ממצלמת הסמארטפון, לא בתוך מסגד. דעאש היה ארגון הטרור הראשון שהבין את מלוא הפוטנציאל של המדיה החברתית, חבריו הניחו את היסודות לטרור מבוסס הרשת".

בהתייחסותו לחופש הביטוי, בר ציין כי הוא בעדו, אך הוא מאמין גם כי יש צורך לנתר את הרשתות החברתיות על מנת למנוע הסתה ברשת. "אנחנו מזהים שבאינסטגרם ובפייסבוק יש הצלחה מסוימת בהורדת תכנים מסיתים, אבל לצערי אני לא יכול להגיד את אותו הדבר על הטלגרם ועל טוויטר".

"בכל הנוגע לבינה מלאכותית, אנחנו מזהים את הפוטנציאל של הטכנולוגיה לפרוץ ולעזור לאנושות, אך גם מזהים את הסיכונים הגדולים שיש ל-AI. בכל הנוגע אלינו, אין שום כוונה להפוך את הבינה המלאכותית לגורם שמקבל החלטות, אבל בתור ‹טייס משנה›, ללא ספק הטכנולוגיה הולכת לעשות מהפכה גם בעולמות המודיעין".

גבי פורטנוי, ראש מערך הסייבר הלאומי, התייחס בדבריו בכנס לפעילות הסייבר ההתקפית של איראן ושל חיזבאללה כנגד ישראל ואמר: "כל מי שמבצע מתקפות סייבר נגד אזרחי ישראל צריך לקחת בחשבון את המחיר שהוא ישלם על כך".

על קבוצת התקיפה MuddyWater המשויכת למשרד המודיעין והביטחון של איראן, שתקפה את הטכניון לפני מספר חודשים אמר: "הקבוצה עובדת לא רק נגד ישראל, אלא תוקפת מטרות אזרחיות במדינות רבות בהן טורקיה, ערב הסעודית, מצרים, מרוקו, הודו, בחריין, עומאן, כווית ועוד". יש לציין כי בשנה האחרונה ניסתה הקבוצה לתקוף גופים נוספים בישראל, רובם ללא הצלחה.

"קהילת הסייבר הישראלית מכירה את פעולות הסייבר של האיראנים מבפנים ומבחוץ, ועובדת לשבש אותה בדרכים שונות. אנשי משרד המודיעין האיראני, אנשים ממשמרות המהפכה האסלאמית וחיזבאללה שמעורבים במבצעי סייבר כנגד ישראל יודעים בדיוק על מה אני מדבר", כך לדבריו.

פורטנוי הוסיף ואמר כי "אני רוצה לחזק את פעילות ארה"ב כנגד האלימות האיראנית ואת הסנקציות שהם השיתו כנגד שני שחקנים איראנים במשרד המודיעין: פרזין כרימי ומג'תבא מצטפוי שייסדו את "אקדמיית ראווין" המאמנת האקרים למטרות זדוניות. כמו כן, עלי חידרי היושב בביירות ומתאם שיתוף פעולה בין איראן לחיזבאללה לשם גרימת נזק לאזרחי לבנון במרחב הסייבר. עבור חלק מהאנשים במשרד המודיעין האיראני, להזיק לאזרחים מהשורה בעולם זה חלק מהשיגרה".

פורטנוי פנה לנציגים הבכירים של קהילת הסייבר הבין-לאומית שישבו באולם ואמר כי "הקהילה הבין-לאומית צריכה לעבוד יחד כדי לעצור אנשים כמו כרימי, מצטפוי וחידרי מפעילותם הזדונית כנגד העולם".

הכנס מגיע בתקופה בה מתגברים ניסיונות התקיפה על ישראל, שהופכים למתוחכמים יותר ויותר, בין היתר עקב ההתפתחות המהירה של כלי בינה מלאכותית המאפשרים להוציא מתקפות סייבר במהירות וכמות שטרם נראתה כמוהן.

המדינה - בריאות, משפט, ביטחון, חינוך וכו', לטובת כלל אזרחי ישראל".

אלוף ערן ניב, ראש אגף התקשוב וההגנה בסייבר בצה"ל, שנאם בכנס, התייחס בדבריו גם כן לתחום הבינה המלאכותית וציין את השפעותיה על שדה הקרב הנוכחי והעתידי: "בלי יסוד דיגיטלי חזק ואפקטיבי, לא ניתן יהיה לנהל מלחמה בשום תחום. בלי בסיס דיגיטלי חזק, לא נוכל לבצע אירועים גדולים".

לדבריו, "הבינה המלאכותית היא תופעה שהולכת וגדלה, בדגש על AI גנרטיבי. מדובר במהפכה המגדילה את יכולותינו ובמקביל גדלה גם ההסתמכות שלנו על תשתית דיגיטלית בכל התחומים. מעריך כי תוך שנים ספורות, כל מרחב הלוחמה יהיה מבוסס מידע ו-AI גנרטיבי"

"בשדה הקרב המודרני, כל אמצעי, כטב"מ, טנק, ספינה וכן הלאה, יכול להעביר מידע לכל אמצעי אחר והכל יהיה מחובר אחד לשני. זה החזון של הקמת מרחב דיגיטלי בשדה הקרב. התחום הדיגיטלי הופך את כל שאר תחומי הלוחמה לחזקים הרבה יותר, באוויר בים וביבשה", סיכם ניב.

בכנס דיבר גם גיא כספי, יו"ר חברת דיפ אינסטינקט, והתייחס לסיכוני סייבר הנוגעים לבינה מלאכותית: "תוך לא יותר מ-15 דקות אפשר לייצר באמצעות Chat GPT קבצים זדוניים והתקפות מתוחכמות ולעקוף את כל מנגנוני ההגנה המוכרים לנו. מי שבנה בחודשים האחרונים על טכנולוגיה של LLM ו-Open AI כפתרון הגנתי - טעה. זו טכנולוגיה מדהימה ללמידת שפה אבל זה מנגנון עצום ואיטי, שלא יכול למנוע מראש מתקפות סייבר במהירות הנדרשת".

עכשיו 14

ראש השב"כ בר חושף: "טכנולוגית ה-AI הוטמעה במכונת הסיכול של הארגון"

ראש השב"כ חשף הבוקר בכנס שבוע הסייבר השנתי באוניברסיטת ת"א כי הארגון בראשותו הוא עומד משתמש בטכנולוגית ה-AI • "זיהינו באמצעותו מספר לא מבוטל של איומים", סיפר בר • מנגד הוא הבהיר: "על מנת לוודא שה-AI יוביל לאבולוציה ולא לרבולוציה, נצטרך שת"פ בין ענקיות הטכנולוגיה לגופי הבטחון"

ראש השב"כ רונן בר נשא הבוקר (שלישי) דברים בכנס שבוע הסייבר השנתי באוניברסיטת ת"א, במסגרתו התייחס לחדירת טכנולוגית ה-ai (הבינה המלאכותית) לזירות רבות בעולם – בהן גם הביטחונית, וחשף כי הכלי הפופולרי הגיע גם לשירות הביטחון הכללי הישראלי

"טכנולוגית ה- ai הוטמעה במכונת הסיכול של שב"כ באופן טבעי. זיהינו באמצעות ה- ai מספר לא מבוטל של איומים", אמר בר והוסיף: "על מנת לוודא שה- ai יוביל לאבולוציה ולא לרבולוציה, נצטרך שיתופי פעולה ופתיחות בין ענקיות הטכנולוגיה לגופי הבטחון ארגוני הבטחון המסורתיים נדרשים להתאים את עצמם למצב החדש, שבו כל אדם זועם עם גישה לאינטרנט עשוי להפוך למפגע, בהחלטה של רגע".

בהמשך הוא הסביר: "גוב האריות, שחוסל בפשיטה של לוחמינו בקסבה, נולד ממצלמת הסמארטפון, לא בתוך מסגד. אנו מצויים בנבכי הרשת ורואים היטב את המתרחש בה: ריגול, טרור, הסתה והשפעה זרה".

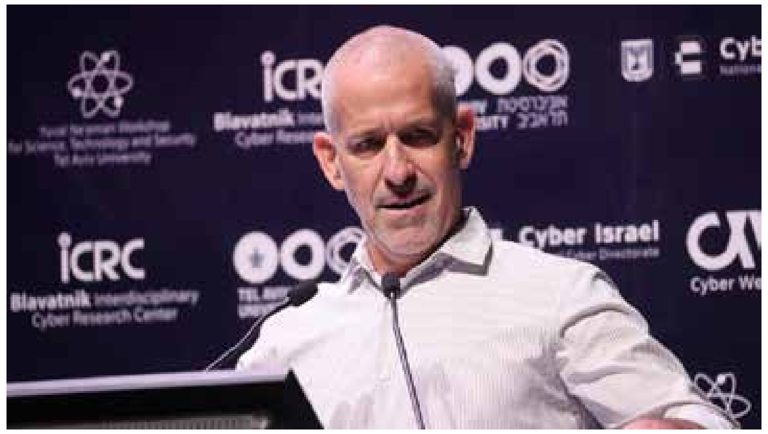
לסיום, אמר ראש השכב כי "הרשת, כמו קיני המחבלים בג'נין ומנהרות הטרור בעזה, אינן מרחב בטוח עבור אויבינו כיפת הברזל שבשב"כ מפתח בסייבר כבר עושה את צעדיה הראשונים, מערך הבריתות מתהווה וגם הוא נכנס כבר לפעולה. אנו כבר משתפים פעולה עם מספר מדינות משמעותיות בתחום ורואים את כיפת ברזל הסייבר העולמית מתחילה לקרום עור וגידים".

מקור ראשון

ראש השב"כ על בינה מלאכותית: "לצערי, אנו לא זריזים כפי שעלינו להיות"

ראש השב"כ רונן בר, דיבר היום (ג›) בכנס שבוע הסייבר השנתי באוניברסיטת תל-אביב. בר סיפר מה קרה כשביקש מ- ChatGPT להסביר לו איך מכינים חומר נפץ מאולתר

הודיה כריש חזוני



"גוב האריות הוא דוגמא לארגון טרור מסוג חדש, טרור דור ה- Z. הארגון אינו אידיאולוגי, קם ברשת, מגייס ברשת ומקבל את התמיכה שלו מהציבור בצורה של לייקים. מאחורי הקבוצה הזאת, נמצאת זרועה הארוכה של איראן. איראן מסמנת ברשת נוער מועד לפורענות, מסיתה, מעבירה להם כספים ומספקת להם ידע ונשק. ככה פשוט", תיאר בר.

עוד התייחס אל הבינה המלאכותית ואל האופן בו מסתייע בה השב"כ, וכיצד נושא ההרצאה שלו השתנה מאז שהוזמן לכנס ועד היום, בר אמר כי לצערו החקיקה איזה זריזה דייה כדי לעמוד בקצב הטכנולוגיה.

"לפני שהגעתי לכאן, ביקשתי מ- ChatGPT שיסביר לי איך להכין חומר נפץ מאולתר. הוא ענה לי מיד: I›m sorry, I can›t assist you with that. התעקשתי ושאלתי את אחת החוקרות בארגון- ‹איך הרעים עושים את זה?›. היא ענתה- ‹בקלות. נסח את השאלה שלך מחדש›. אני לא ארחיב, אך בסיומו של צ›אט קצר, ה- ChatGPT כתב טקסט שכלל הסבר מאוד מדויק – אילו חומרים נדרשים, איך לשקול ולערבב אותם וממה צריך להיזהר".

הוא תיאר כי דעא"ש היה ארגון הטרור הראשון שהבין את מלוא הפוטנציאל של המדיה החברתית. הם הניחו את היסודות לטרור מבוסס הרשת. "בשנה שעברה ספגנו פיגוע כזה בבאר שבע. אדם שצרך ברשת תכני דעא"ש מסיתים ומסוכנים (תוכן, שאגב, חוקי בישראל), הושפע עמוקות, הקצין באחת ורצח 4 אנשים עם סכין ומכונית. אנחנו לא ידענו שהוא עומד לבצע פיגוע. אשתו לא ידעה שהוא עומד לבצע פיגוע. אני בספק אם הוא ידע זאת, מספר שעות לפני המעשה. זוהי רק דוגמה אחת לחשיבות עדכון החקיקה לפי קצב השתנות הטכנולוגיה. לצערי, אנו לא זריזים כפי שעלינו להיות.

"מתחילת 2022 טיפלנו במעל ל- 600 פעילים, תומכי דעא"ש בישראל. רבים מהם צרכו תכנים דומים- אלימים ומסוכנים ברשתות החברתיות ובמעמקי הרשת. חלקם היו רגע לפני יציאה לפיגוע. אלה נוספו לכ- 800 פיגועים משמעותיים שסיכלנו באותה תקופה. למספר מדאיג מתוכם, אחיזה ברשת- פוסט, השראה, ידע או קבוצה חברתית. המגמה ברורה. ארגוני הביטחון המסורתיים נדרשים להתאים את עצמם למצב החדש, שבו כל אדם זועם עם גישה לאינטרנט עשוי להפוך למפגע, בהחלטה של רגע".

לגבי הסיכול באמצעות בינה מלאכותית, אמר כי "לשב"כ ול- AI תכונה משותפת עיקרית – אנחנו מתפרנסים מחיפוש אנומליות. ניתן לומר כבר היום: זיהינו באמצעות ה- AI מספר לא מבוטל של איומים. כשליש מעובדי הארגון הם נשות ואנשי טכנולוגיה. גם לעובדי השטח שלנו יש יותר אוריינות טכנולוגית. טכנולוגיה למבצעים, כמו גם מבצעים טכנולוגיים, הופכים לנתח משמעותי יותר ויותר בפעילות שלנו. הבנו שלא נוכל לנצח במלחמה הזאת באמצעות מקלות ואבנים. אנו מזהים את האיומים, אך גם רואים את ההזדמנויות שהאינטליגנציה המלאכותית מביאה עמה. כיפת הברזל ששב"כ מפתח בסייבר כבר עושה את צעדיה הראשונים, מערך הבריתות מתהווה וגם הוא נכנס כבר לפעולה. הסכמי אברהם, יחד עם הסכמי השלום הוותיקים יותר במזרח התיכון, יכולים להוות בסיס איתן לברית אזורית של הגנה בסייבר. אנו מזמינים את כל המדינות שרואות עצמן חלק מהגוש המתון וחפץ החיים בעולם להצטרף לגוף הגנת סייבר משותף", דברי בר.

כיפה

ראש השב"כ שאל את ChatGPT איך מכינים חומר נפץ - זה מה שקרה

רונן בר הסביר מהן הסכנות שמעמידה הבינה המלאכותית לביטחון ישראל - וחשף כיצד בשב"כ מעוניינים לגייס את הטכנולוגיה כדי להגן על המדינה מפני הסתה ואיומים

ראש השב"כ, רונן בר, נאם היום (ג') במסגרת שבוע הסייבר באוניברסיטת תל אביב והסביר אילו אתגרים מודיעיניים וביטחוניים מעמידה טכנולוגיית הבינה המלאכותית, וכיצד מדינת ישראל מתכננת להילחם בכך ואף לגייס את טכנולוגיית ה- AI לטובת הגנה על ביטחון המדינה.

ראש השב"כ הדגים את הפשטות שבה הבינה המלאכותית יכולה להיות מנוצלת לצרכי טרור, "לפני שהגעתי לכאן, ביקשתי מ- ChatGPT שיסביר לי איך להכין חומר נפץ מאולתר", אמר, וסיפר כיצד באמצעות תמרון השאלות, הצ<אט נתן לו את כל המידע שביקש, בפירוט ודיוק.

"גוב האריות נולד ממצלמת הסמארטפון, לא בתוך מסגד"

עוד תיאר את ההשלכות הביטחוניות של השימוש בבינה המלאכותית על ידי גורמי טרור: "ארגוני הבטחון המסורתיים נדרשים להתאים את עצמם למצב החדש, שבו כל אדם זועם עם גישה לאינטרנט עשוי להפוך למפגע, בהחלטה של רגע", מאר, וטען כי איראן יודעת לנצל זאת היטב. "גוב האריות, שחוסל בפשיטה של לוחמינו בקסבה, נולד ממצלמת הסמארטפון, לא בתוך מסגד", הוסיף ואמר, והזכיר את הפיגוע בבאר שבע בשנה שעברה, בו נרצחו 4 בני אדם - כתוצאה מהשפעות ההסתה ברשתות על המחבל.

אולם, ניתן להשתמש בטכנולוגיה גם כדי לגבור על האיומים הללו: "טכנולוגית ה- AI הוטמעה במכונת הסיכול של שב"כ באופן טבעי. זיהינו באמצעות ה- AI מספר לא מבוטל של איומים", סיפר ראש השב"כ והבהיר כי "על מנת לוודא שה- AI יוביל לאבולוציה ולא לרבולוציה, נצטרך שיתופי פעולה ופתיחות בין ענקיות הטכנולוגיה לגופי הבטחון".

בתוך כך, בר ציין כי ישראל מפתחת "כיפת ברזל" מבוססת סייבר, שתגן על הרשתות מפני תכנים מסיתים ומידע שעלול לפגוע במדינה, כדוגמת שיטות לייצור תחמושת. "כיפת הברזל ששב"כ מפתח בסייבר כבר עושה את צעדיה הראשונים, מערך הבריתות מתהווה וגם הוא נכנס כבר לפעולה. אנו כבר משתפים פעולה עם מספר מדינות משמעותיות בתחום ורואים את כיפת ברזל הסייבר העולמית מתחילה לקרום עור וגידים".

"הבעת הפנים של אשתי הבהירה לי - בשימוש לא נכון ה- AI הוא טכנולוגיה מסוכנת"

לסיכום, סיפר אנקדוטה משעשעת מחייו: "כשנתקלתי לראשונה בכלי ה- AI, קיוויתי שהוא אכן יכול לתת תשובה גם לשאלות הקשות ביותר. ולכן, שאלתי דבר פשוט: "?What should I buy for my wife>s birthday present", סיפר. "הצ<אט הציע שאקנה זר ורדים אדומים. עשיתי כמצוותו והגעתי הביתה נרגש, בתקווה שאולי הפעם אצליח להביא את המתנה הנכונה. הבעת הפנים של אשתי הבהירה לי דבר אחד- בשימוש לא נכון ולא מבוקר, ה- AI הוא טכנולוגיה מסוכנת מאין כמותה!"

בחדרי חרדים
bhol.co.il
האתר החרדי הגדול בעולם

"הבינה המלאכותית עלולה לערער את היסודות ולהשפיע על כלל האנושות"

מבקר המדינה הודיע כי יפתח בביקורת משותפת עם מדינות מובילות על מוכנות לעידן ה-AI | "לצד היתרונות הרבים של הבינה המלאכותית, היא טומנת בחובה גם סכנות להתעצמות ארגוני טרור ופשיעה", אמר

צביקה סגל

מבקר המדינה מתניהו אנגלמן השתתף היום (רביעי) בוועידת "שבוע הסייבר" של אוניברסיטת תל אביב. בדבריו חשף המבקר, המכהן גם כסגן נשיא ארגון המבקרים האירופאי (EUROSAI), כי משרדו יתחיל בביקורת על מוכנות המדינה לעידן הבינה המלאכותית (AI). הביקורת תיעשה בשיתוף פעולה עם גורמים נוספים באירופה כדוגמת מבקר האיחוד האירופי, ומבקרי המדינות של בריטניה, גרמניה ומדינות רבות נוספות.

הביקורת תתמקד בשלושה היבטים בנוגע לפעולות הממשלה ולהיערכותה: התמודדות עם סיכוני הבינה המלאכותית בהיבט הטכנולוגי, קידום רגולציה וחקיקה, ויישום כלי בינה מלאכותית במערכות ציבוריות-מדינתיות.

לדבריו, "הבינה המלאכותית עשויה להביא לכדי התקדמות טכנולוגית רחבת היקף בתחומים רבים אך לצדה קיימים סיכונים רבים ובהם "פייק ניוז", שימוש ב-AI ע"י גורמי טרור ופשיעה וההיערכות לשינויים הדרמטיים בשוק העבודה. בנושא הטכנולוגי נבדוק האם הממשלה מוכנה לטכנולוגיה החדשנית בהיבטי הממשל, יכולות המחשוב, ההון אנושי ועוד; בסוגיית הרגולציה והחקיקה נבדוק כיצד מגינה הממשלה על אזרחיה ועל עצמה על ידי הגבלת השימוש בטכנולוגיית AI שעלולה לגרום להשפעות שליליות ולחשוף את הציבור לסכנות. ההיבט השלישי הוא יישום בינה מלאכותית במערכות ציבוריות-מדינתיות. במסגרתו נבדוק האם וכיצד בינה מלאכותית מוטמעת בתוך מערכות המדינה - בריאות, משפט, ביטחון, חינוך וכו'.

כמבקר המדינה אני רואה חשיבות משמעותית בביצוע ביקורת מקיפה בתחום הבינה המלאכותית וסיכוניה. עולם הביקורת רואה בסיכוני בינה מלאכותית סיכון מרכזי. האתגרים הכרוכים בהתמודדות עם העניין מורכבים והם דורשים, בין היתר, שיתוף פעולה רציף בין מדינות, להתמודדות מיטבית עם סיכוני בינה מלאכותית. לצד היתרונות הרבים של הבינה המלאכותית, היא טומנת בחובה גם סכנות גדולות להתעצמות ארגוני הטרור והפשיעה.

היא עלולה לערער את היסודות עליהם אנחנו נשענים ולהשפיע על כלל האנושות. על מבקרי המדינות לבדוק שמדינות המערב, וישראל בתוכן, מוכנות לעידן ה- AI. אנו במשרד מבקר המדינה מתחייבים להמשיך ולהתייחס לנושא משמעותי זה ביתר שאת, לטובת אזרחי ישראל והעולם כולו".

ערוץ 7

ראש השב"כ: כל אדם עם גישה לאינטרנט יכול להפוך למחבל

ראש השב"כ רונן בר הבהיר כי "הרשת, כמו קיני המחבלים בג>נין ומנהרות הטרור בעזה, אינן מרחב בטוח עבור אויבינו".

ראש השב"כ רונן בר התייחס הבוקר (שלישי) לטכנולוגיית ה- AI וחשף כי בעזרתה השב"כ זיהה מספר לא מבוטל של איומים.

"טכנולוגית ה-AI הוטמעה במכונת הסיכול של שב"כ באופן טבעי", אמר בר בכנס שבוע הסייבר השנתי באוניברסיטת ת"א.

לדבריו, "זיהינו באמצעות ה-AI מספר לא מבוטל של איומים. על מנת לוודא שה-AI יוביל לאבולוציה ולא לרבולוציה, נצטרך שיתופי פעולה ופתיחות בין ענקיות הטכנולוגיה לגופי הבטחון".

בנוסף אמר כי "ארגוני הבטחון המסורתיים נדרשים להתאים את עצמם למצב החדש, שבו כל אדם זועם עם גישה לאינטרנט עשוי להפוך למפגע, בהחלטה של רגע".

בר נתן דוגמה: "גוב האריות, שחוסל בפשיטה של לוחמינו בקסבה, נולד ממצלמת הסמארטפון, לא בתוך מסגד".

"דעא"ש", לדבריו, "היה ארגון הטרור הראשון שהבין את מלוא הפוטנציאל של המדיה החברתית. הם הניחו את היסודות לטרור מבוסס הרשת".

הא הבהיר: "אנו מצויים בנבכי הרשת ורואים היטב את המתרחש בה, ריגול, טרור, הסתה והשפעה זרה. הרשת, כמו קיני המחבלים בג>נין ומנהרות הטרור בעזה, אינן מרחב בטוח עבור אויבינו"

"כיפת הברזל ששב"כ מפתח בסייבר כבר עושה את צעדיה הראשונים", אמר, "מערך הבריתות מתהווה וגם הוא נכנס כבר לפעולה. אנו כבר משתפים פעולה עם מספר מדינות משמעותיות בתחום ורואים את כיפת ברזל הסייבר העולמית מתחילה לקרום עור וגידים".

הוא סיפר כי לפני הגעתו לכנס, "ביקשתי מ-ChatGPT שיסביר לי איך להכין חומר נפץ מאולתר. הוא ענה לי מיד: "I>m sorry I can>t assist you with that".

התעקשתי ושאלתי את אחת החוקרות בארגון: <איך הרעים עושים את זה?>. היא ענתה- <בקלות! נסח את השאלה שלך מחדש!>. אני לא ארחיב, כדי לא לתת לאף אחד רעיונות, אחרי הכל, אנחנו אלה שצריכים לעצור אותם. אני כן אומר שבסיומו של צ>אט קצר, ה- ChatGPT כתב טקסט שכלל הסבר מאוד מדוייק- אילו חומרים נדרשים, איך לשקול ולערבב אותם וממה צריך להזהר".

"מתחילת 2022 טיפלנו במעל ל- 600 פעילים, תומכי דעא"ש בישראל. רבים מהם צרכו תכנים דומים- אלימים ומסוכנים ברשתות החברתיות ובמעמקי הרשת. חלקם היו רגע לפני יציאה לפיגוע", חשף בר.

כאן 11

כתבת הטלוויזיה המיוחד עם כריס ופרופ' בן ישראל: "החברה שמבטיחה: מטוס שיביא אתכם מישראל לניו יורק - בחמש שעות"

Cyber Week

June 26th-29th, 2023

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 · Israel Export Institute · Tel Aviv-Yafo תל אביב-יפו

עכשיו 14

ראש השב"כ חושף: בינה מלאכותית לסיכול טרור

גלצ

ראיון מיוחד של פרופ' איציק בן ישראל עם פתיחת שבוע הסייבר

כאן ב

ראיון מיוחד של פרופ׳ איציק בן ישראל עם פתיחת שבוע הסייבר

כאן ב

דיווח על דבריו של הבכיר מאיחוד האמירויות

כאן ב

מתוך כאן מורשת: פרופ׳ יצחק בן ישראל, ראש מרכז הסייבר

גלצ

ראיון עם תא״ל במיל׳ רמי אפרתי על השתתפותו בכנס