

Global Cyber Bi-Weekly Report by INSS October 15 2018

Editor-in-chief: Gabi Siboni, **Editor:** Hadas Klein, Gal Perl Finkel

Contributors: Simon Tsipis, Anna Danilova, David Libin, Gal Sapir, Michal Beit Halachmi

ISRAEL

Two Israeli firms chosen to aid New York City in quest to be cybersecurity “global leader”

New York City is launching an initiative to improve its cybersecurity sector and two Israeli institutions are among the chosen institutions. SOSA, founded in 2014, brings together start-ups and multinational corporations and investors from all over the world. The Jerusalem Venture Partners (JVP) was founded in 1993 and has created and invested in over 120 companies in Israel, the United States, and Europe. The Global Cyber Center in Chelsea, part of the initiative, will be set up by SOSA, and JVP will run the first international cybersecurity investment hub in SoHo in the city. The New York City Economic Development Corporation unveiled its plan to transform New York City “into a global leader of cybersecurity innovation and talent to combat one of the world’s greatest threats.” The initiative comes as cybersecurity attacks are increasing globally both in number and intensity.

<https://bit.ly/2QtBrKr>

Israel Aerospace Industries teams with Tech Mahindra on cybersecurity

Software major Tech Mahindra, an Indian multinational provider of innovative and customer-centric information technology, announced a strategic partnership with ELTA Systems Ltd. to provide next-generation cyber solutions and services globally. The company, a group and subsidiary of Israel Aerospace Industries (IAI), will initiate a partnership to enable both companies

to design and deliver AI and machine-learning analytics together. ELTA's IAI Cyber Division manager Esti Peshin stated that, "We are confident that Mahindra's experienced cybersecurity professionals will equip IAI with a sustainable competitive advantage, improving our ability to scale rapidly and prevent cyberattacks with cutting-edge cybersecurity solutions."

<https://bit.ly/2IGHqsQ>

Israeli cybersecurity company Hysolate raises \$18 million

Hysolate, an Israeli cybersecurity company launched by Team8, announced it has received \$18 million in funding by Bessemer Venture Partners and Innovation Endeavors. The company will use the funding to accelerate the adoption of the Hysolate Platform, which fully protects endpoints from cyberattacks while boosting end-user productivity. Additionally, Hysolate will use the funds to invest in expanding its global market presence. Hysolate was founded by CEO Tal Zamir, a veteran of an elite Israeli cyber unit, and Dan Dinnar, former CEO of HexaTier, which was acquired by Huawei in September, 2016.

<https://bit.ly/2OFE2UA>

Israel Securities Authority starts using blockchain for cybersecurity

The government's Israel Securities Authority (ISA) started using blockchain technology to improve cybersecurity within its operating systems to meet the current information security challenges. The ISA said the change to blockchain "adds another layer to ensuring the credibility of the information relayed to the supervised bodies." Blockchain is known as the technology that reinforces digital cryptocurrency, such as Bitcoin, through a system allowing digital information to be distributed but not copied. An additional update of two more systems will be done in the future to secure an online voting system and later in Magna, which is used to record all the reports by bodies under ISA's supervision.

<https://bit.ly/2DVrXGn>

UNITED STATES

Support for “hack back” grows after Trump’s pledge to get aggressive in cyberspace

The recently released national cyber strategy postulates a new era of US response to threats to cybersecurity: a pledge to implement more aggressive and offensive actions in cyber operations. Producing a growing reception of private companies permitted ability to “digitally retaliate” or ‘hack back’ to cyberattacks. Lawmakers have alluded to amending the Computer Fraud and Abuse Act, a law banning the defensive and offensive dual-type response mechanism in the United States. Bearing light on these efforts, although denied, reported earlier this summer, Madiant infiltrated Chinese hackers by accessing their network and activating the cameras on their laptops. Hack back opponents response seem to range from condemning the capability to suggesting a tolerance for particular private firms such as defense contractors, and critical infrastructure services.

<https://bit.ly/2Esy8ls>

Facebook says Russian firms “scraped” data, some for facial recognition

In the wake of the Facebook crisis, beginning with the Cambridge Analytica incident exposing the data of 87 million users in an effort to manipulate the 2016 US elections, followed by the company’s biggest data breach in its fourteen years, jeopardizing 30 million users, has seemingly progressed. In its most recent announcement, Facebook removed sixty-six accounts, pages and apps associated to SocialDataHub and Fubutech, Russian firms that design facial recognition software for their government. Facebook found the companies in violation of its policies for “scraping” data or pulling information from its network. Both SocialDataHub and Fubutech contest the allegations, stating the technique was only used through Google on Russian citizens with advanced permission, in the training of journalist students—some who practiced the technique on their classmates’ Facebook profile—and to

facilitate credit assessment capacity for its clients of banks and insurers. Facebook has recognized the larger issue at hand, of third-party apps access to its users' data.

<https://nyti.ms/2pSQL87>

There is a serious threat to the supply chain, says Pentagon

The current viral news involving Supermicro, the Taiwanese-American information technology company that operates in China, is that it unknowingly manufactured tampered hardware installed with surveillance chips used in thousands of servers by Apple, Amazon, and other US companies. It demonstrates the magnitude of the threat concerning adversary infiltration and cyber espionage efforts on the US supply chain and networks. Reportedly, hostile actors associated with a unit in the People's Liberation Army installed the chips in the motherboards during the assembly process, facilitating the back-door mechanism to US companies networks. A new Pentagon report highlights the lack of resolve on the "foundation sector"; the report calls attention on the non-existent nature of cybersecurity embedded norms, standards, and sufficient compliance in small-to-medium-sized manufacturers. China is mentioned a hundred times throughout the report, accused extensively of appropriating sensitive material, challenging the resilience of trade secrets and the notion that they could reach the hands of China, Russia, and North Korea. Calling attention to the Supermicro incident, as well as to the Naval Undersea Warfare Center breach, resulting in 614 gigabytes stolen, this is a pressing issue, reinforced by the estimated 51 percent of components shipped to US companies that originate in China and has triggered an investigation in Washington.

<https://bit.ly/2yiLprt>

EUROPE

Insiders "cause 73 percent of UK's data breaches," says risk report

The 2018 IT Risks Report from Netwrix has found that while 50 percent of UK respondents consider external hackers as “the most dangerous threat actors” in terms of being the source of a potential data breach, the response results indicate that “insiders” are the cause of security incidents in 73 percent of the cases. The report shows that the biggest risk is to regular business users (33 percent), mid-level managers (22 percent), departing/departed employees (22 percent), and members of an organization’s IT team (17 percent).

<https://bit.ly/2yCGMbc>

Supercomputers: EU to develop high-performance data infrastructures

Member states from across the European Union agreed on September 28 to take a leading role in developing high-performance computers on the continent, an area where Europe has fallen seriously behind China and the United States. High-performance computing involves the large-scale computation of data that cannot be performed by general-performance computers. Currently, the EU provides about 5 percent of supercomputing resources worldwide but consumes one-third of them, and member states have long been in dire need of expanding their supercomputer capacities.

<https://bit.ly/2Cj8Bse>

DASA new competition: Behavioral Analytics

This Defence and Security Accelerator (DASA) competition is seeking proposals that can help UK Defence and Security to develop capability in “Behavioral Analytics.” DASA is looking for scientific and technological solutions that can provide context-specific insights into the “how” and “why” of individual, group, and population behavior, enabling predictions about how they are likely to act in the future.

<https://bit.ly/2NGiqm4>

One in ten reported malicious emails

New findings from Cofense have revealed that one in ten reported emails in 2018 were malicious, with more than 50 percent of those linked to fraudulent attempts to gather login and system information from the email users, known as credential phishing. As detailed in its report "The State of Phishing Defense 2018: Susceptibility, Resiliency, and Response to Phishing Attacks," the firm analyzed more than 135 million phishing simulations, 800,000 reported emails and nearly 50,000 real phishing campaigns targeting organizations in twenty-three industries ranging from healthcare, financial services to manufacturing. Key findings discovered that 21 percent of reported crimeware emails contained malicious attachments while the term "invoice" was one of the most-used phishing subjects, appearing in six of the ten most effective phishing campaigns this year.

<https://bit.ly/2Os2qcX>

Deluge of student devices putting campus networks under growing threat

Securing networks used by students and faculty has become more difficult in the past two years due in part to the proliferation of connected devices, according to 81 percent of campus IT professionals surveyed. Over 600 students, IT professionals, and staff from higher education institutions in the United States, United Kingdom, and Germany were surveyed by Infoblox for the report entitled "Defending Networks at Higher Learning Institutions—Heroes Needed." The report found that networks at higher education institutions are becoming increasingly complex, making them more vulnerable to attack. While two years ago students mainly brought laptops and smartphones with them, in the era of the internet of things, students are using tablets (61 percent), smartwatches (27 percent), and gaming consoles (25 percent) on campus, which has led to a dramatic increase in the number of devices connecting to networks.

<https://bit.ly/2Pz8wEC>

Hungary increases its scientific cooperation with NATO

Scientists and other experts from NATO and Hungary discussed future projects of cooperation at the NATO Science for Peace and Security (SPS) Programme Information Day held in Budapest on October 11, 2018. Hungary is currently leading an SPS project in the area of chemical, biological, radiological, and nuclear (CBRN) defense. The multi-year initiative aims to develop a cutting-edge sensor to detect bio-toxins, including in water and food. A number of young scientists, including from Ukraine, are contributing to the research effort, also helping them to kick-start their career.

<https://bit.ly/2ITMHx7>

RUSSIA

Western intelligence agencies: We are in the middle of Russia's global attack

Western intelligence admits that the Russian military intelligence agency, GRU, and its agents are involved in what seems as a global net of secret operations, from assassinations, to cyberattacks. Leading European and American intelligence agencies have discovered GRU's traces in Skripal's poisoning, as well as in attempts to hack the World Anti-Doping Agency in 2017, the Democratic National Committee (DNC) in 2016, the theft of emails from a UK-based tv station in 2015, and hacking the Organization for the Prohibition of Chemical Weapons (OPCW) in April this year. Hacking soft malware, such as BadRabbit, Fancy Bear, Sofacy, Pawnstorm, Sednit, CyberCaliphate, Cyber Berkut, Voodoo Bear, and BlackEnergy Actors all seem to lead to GRU's cyber department, Britain's Cyber Intelligence Agency said.

<https://reut.rs/2q057nv>

Facebook and Twitter reveal how much Russia invested in ads to manipulate opinion

During the Senate hearings of high-level executives from Facebook and Twitter, Mark Zuckerberg admitted that his company had made about

\$100,000 profit from ads placed by the Internet Research Agency, a Russian troll factory, during the US elections.

<https://nyti.ms/2IVgFB0>

Britain intelligence: Russian GRU put UK TV channel under their complete control

Britain claims that in 2015, Russian agents, affiliated with the military intelligence service GRU, hacked the Islam Channel, a UK-based Islam-focused tv station. The agency said that the station fell under complete control of the GRU hacking team, without the station's executives knowing it.

<http://bit.ly/2Etj87g>

More sanctions against Russia discussed in European Union due to GRU's cyberattacks

A few days after the British Foreign Office stated that London had assessed "with high confidence" that the Russian military intelligence service was "almost certainly" responsible for a series of cyberattacks on political institutions, media outlets, and infrastructure across the globe, including Britain, British and German leaders are planning to enhance their sanctions' policy against Russia.

<http://bit.ly/2EiHvnK>

United Kingdom to decide to launch preventive cyberattack against Russian infrastructure

The British Ministry of Defense is considering the possibility of conducting cyberattacks on power supply facilities in Russia in the event of "Moscow's aggression," according to the Sunday Times. UK authorities decided that a massive cyberattack could be the only alternative to the use of weapons in response to the "Russian aggression."

<http://bit.ly/2PtqgRU>

British military exercises possible cyberattack on Russia in case of major conflict

During the recent UK military drill in Oman, UK cyber forces practiced cyberattacks on Russia, as a response to possible Russian aggression against Britain and its allies. The United Kingdom's main military scenario is to shut down Russian electrical infrastructure, putting Russia into a full blackout, which would allegedly complicate its own military activity.

<http://bit.ly/2q07ald>

ASIA PACIFIC

China's new cyber security rules pose new challenges to US companies

The new rules, which will go into effect on November 1, give the Chinese government power to pursue a company's records, and remotely access a company's networks that they deem as a danger to Chinese national security. According to experts from Sidley Austin, a company focused on privacy and data security, the new regulations include not only personal identifiable information but also trade secrets that often overlap as well as sensitive information on cultural and political issues.

<https://goo.gl/gWxrLw>

Australia will train Indonesia personnel in Cyber Security

During the meeting between Australian defense minister Christopher Pyne and his Indonesian counterpart, Ryamizard Ryacudu, in Bali on October 10, the two agreed on cooperation in cyber security, and how Australia can take an active role in the "Our Eyes" initiative, a program established in January between Indonesia, Brunei, Malaysia, Singapore, Thailand, and the Philippines. Australia already cooperates with Indonesia in analyzing shared information in regards to counterterrorism, but the meeting focused on expanding cooperation in the cybersecurity field, with the Indonesian defense minister stating that "Australia has better technology."

<https://goo.gl/VHYTMg>

State Bank of Mauritius recovers 90 percent of lost funds after major cyber fraud

Mumbai police investigation reveals that hackers compromised the SWIFT system of the State Bank of Mauritius (SBM). The hackers remitted RS 147 crore (nearly 20 million dollars), in different bank accounts in London, Paris, and New York. Police said that the hackers used malware to hack the system on October 1. After the money was remitted, the hackers or their accomplices withdrew money simultaneously on October 2–3. On October 5, SBM requested all overseas accounts to block all payments; however the hackers had managed to already withdraw around Rs 30 crore (around 4 million dollars). The bank claims it only lost Rs 19 crore, and is working on additional proactive measures to prevent further damage. The investigation is ongoing.

<https://goo.gl/dX5L2a>

MIDDLE EAST

Analysts: Cyberattacks a “real threat” to GCC businesses

The Gulf Cooperation Council (GCC), the regional intergovernmental political organization union of Gulf states, noticed an increase in cyberattacks threatening businesses operating in the region. Security experts have called for more data protection to prevent businesses, consumers, and governments from being victimized by a varied range of cybercrimes, including malware emails, ransomware, and most recently crypto jacking. Nations like Dubai and Saudi Arabia are moving towards greater protection by launching a cybersecurity strategy and setting up the National Authority for Cyber Security. Haider Pasha, chief technology officer for Symantec Middle East, said “you need to really understand where your sensitive data is, where the assets are and have a robust security strategy or framework that you can abide by. I see that happening more and more within Saudi Arabia and the UAE.”

<https://bit.ly/2A3GvzW>

Data security emerges as top priority for financial sector

Top finance executives and CFOs in banks and financial institutions are changing their top priority to data security and privacy, according to a survey by the global consulting firm Protiviti. A growing anxiety over possibilities of data breaches leading to billions of dollars in losses and reputational damage has caused financial institutions to change its focus from regulatory and tax-related issues to data theft. In 2017, the estimated losses on account of data theft and fraud in the global financial sector were estimated to be approximately \$957 million, according to a report by Information Age.

<https://bit.ly/2CbuQAG>

Sophos signs up Ingram Micro to deliver next generation of cybersecurity solutions

Cooperation between information technology distributor Ingram Micro and cybersecurity company Sophos will lead to the next generation of cybersecurity solutions to protect the Gulf Cooperation Council (GCC), Egypt, Jordan, Lebanon, Libya, Iraq, and Yemen. Sophos distributes networks and endpoints, including web, email, and server and mobile security through its wide network of resellers across the region. "Ingram Micro strongly believes in empowering organizations with best-in-class cyber-defense capabilities. With cyber threats evolving and changing daily, organizations of all sizes need training, services, consultancy and technology that's on the frontline of developing highly effective security solutions," said Ingram Micro Cyber Security Director Marc Kannis.

<https://bit.ly/2IPpOuK>