Global Cyber Bi-Weekly Report by INSS November 1 2018

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

Contributors: Simon Tsipis, Anna Danilova, Gal Sapir, Michal Beit Halachmi, Stefan Weenk

ISRAEL

Israel's Team8 launches $85 million cybersecurity and data fund

Team 8, Israel's think-tank and cybersecurity company creation platform specializing in cyber resilience and data science, gathered $85 million through investors, including Walmart, Airbus, Barclays, and Scotiabank. Its existing investors, Cisco, Nokia, and Temasek also invested in the new fund. Team 8 launched the foundation to build eight cybersecurity and data companies over the next five years. The company, founded by former leaders of the intelligence unit 8200 of the Israel Defense Forces (IDF), raised more than $260 million through investments.

https://nyti.ms/2Q60OlQ

Revealed: Israel's cyberspy industry helps world dictators hunt dissidents and gays

An investigation done by independent daily newspaper Haaretz reveals Israel has become a global leading exporter of tools for spying on civilians. The investigation also revealed that dictators around the world are using the technology to eavesdrop on the gay community after those systems were installed. Azerbaijan and Indonesia used the spyware product of Verint to create a database of LGBT rights activists for surveillance and it was also used against religious minorities. Another case was that of Ahmed Mansoor, a human rights activist from the United Arab Emirates, who is currently serving a ten-year prison sentence for publishing critical posts about the regime on

social networks. The Pegasus spyware, created by NSO of Haifa, was used to access his iPhone and his personal information.
https://bit.ly/2J4UgRT

Secretive crackdown on fake profiles shows Israel wide open to election meddling

Israel's National Cyber Directorate joined forces with online social media giants to address and prevent the influence of fake Facebook profile accounts created to spread fake information about Israeli political candidates. The active efforts to prevent election interference came after the social media interference during the US presidential elections in 2016. Israel's cyber agency refuses to give detailed information about the crackdown on fake profiles, which raises concerns about its transparency, and potential political manipulation. Members of Knesset said that the crackdown occurred too late to safeguard Tuesday's elections and to prevent any influencing of the vote. The head of the directorate's personal protection unit, Erez Tidhar, acknowledged that Israeli political parties were behind some of the fake profiles.
https://bit.ly/2AAryWk

UNITED STATES

Inside the Pentagon's struggle to build a cyber force

In line with the 2018 Defense Science Board report, the Pentagon has prioritized recruiting cyber talent to fill 8,300 positions to contend with related threats and effectively structure a "digitally cohesive unit." As of 2016, only 46 percent of cyber associated positions in the Air Force were filled. Challenging the low retention level of US military efforts is the competition for talent with the private sector, as well as ongoing issues with military cyber linked training. In response, the Department of Defense announced the opening of the Tatooine workspace in Augusta, Georgia, a partnership between civilian and military officials collaborating in "start-up"-like spaces,

utilizing private-sector technology and tools related to cyber issues. Projects include pursuing aggressors in the Pentagon network, designing detection technologies, and a training program for "cyber soldiers." This past summer, the US Cyber Command also demonstrated extensive and new hiring tactics, suggestive of a modified future in the national forces regarding access to human capital and the change in the ratio of civilian-military officials.
https://bit.ly/2yFyXCr

Mirai co-author gets house arrest, $8.6 million fine

In Trenton, New Jersey, US District Judge sentenced Paras Jha, 22, responsible for a series of DDoS attacks, to six months of house arrest, five years parole, 2,500 hours of community service, and a restitution fine of nearly $9 million. Jha will serve an additional sentence from 2017, when he was found guilty of violating the Computer Fraud & Abuse Act, for his role in the Mirai botnet operation, in which he was assisted by Josiah White, 21, and Norman Dalton, 22. The Mirai DDoS attacks took place between November 2014 and September 2016 and were launched against Rutgers University. The attacks caused the shutdown of the central authentication server, which maintained portals accessed by staff, faculty, and students. The malware compromised over 100,000 devices, including routers utilized to spread the botnet and create a larger traffic routing network. The breached devices were part of a bigger scheme involving deceitful advertisement referred to as "click-fraud," generating millions of dollars. Before the attacks, Jha exposed the botnet source code in a forum, facilitating the reproduction and utility of the malware in several other attacks. A case in point was Mirai #14, created by Daniel Kaye, a British national sentenced in Germany early 2017 and who was referred to as "BestBuy" and "Spiderman" and was responsible for the breach of 1.25 million Deutsche Telekom routers.
https://bit.ly/2qiS6oZ

Hackers breach healthCare.gov system, get data on 75,000 people

The Centers for Medicare and Medicaid Services announced the breach of an official computer system associated with the health care program initiated by former president Barack Obama, compromising the sensitive data of about 75,000 people. The system was shut down and is set to be restored by the first of November when registration begins for the new year. Although only the portals of the insurance agents and brokers were hacked, the threat of vulnerability extends to the collective ten million people receiving health care coverage under the Affordable Care Act managed through HealthCare.gov, in addition to the additional unknown number of applicants who signed up and were rejected or terminated the process. The risk lies in the substantial amount of personal information required, such as social security number, income, and citizenship status.
https://bloom.bg/2EQDKGp

RUSSIA

First person arrested in Robert Mueller's Russian-US cyber-crime investigation

US authorities arrested a Russian national, who, according to the charge, participated in the Russian intervention of US politics by attempting to influence the elections' outcomes. The person is Elena Khusyaynova, who, according to the investigation, plays a key financial role in a Kremlin-backed plan to conduct "information warfare" against the United States, including ongoing attempts to influence the upcoming congressional elections. Eventually, according to the sources connected to the investigation, both attempts to influence the US elections—the presidential, as well as the congressional—are sponsored and executed by the same source, and directly connected to Russia's President Putin. The arrest comes as a result of Special Counsel Robert Mueller's separate investigation of alleged Russian meddling

in the 2016 US presidential elections, and Elena Khusyaynova is the first person charged with the crime.

https://reut.rs/2JlKr26

US investigation: Russian methods of interference revealed

According to the US investigation, among other techniques, Russian-backed "trolls" used social media to call the late Senator John McCain of Arizona an "old geezer" and Special Counsel Robert Mueller "a puppet of the establishment." President Donald Trump, the trolls were told to say, "deserves a Nobel Peace Prize" for meeting with the North Korean leader Kim Jong Un. The messaging strategy mimicked the overheated rhetoric that the St. Petersburg firm, financed by an ally of Russia's President Vladimir Putin and closely tied to Russian intelligence, employed to considerable effect during the 2016 presidential elections. More than 470 Facebook pages where opened by Russian-backed trolls. The Russians used PayPal accounts and utilized a complex network of shell companies to finance the operation. According to the investigations' assessment, the budget for the project exceeded 73 million Russian rubles—or roughly $1.2 million—per month.

http://bit.ly/2OgxBmE

Russian bloggers being mysteriously assassinated by the same head of Putin's "troll factory"

According to the Telegraph sources, Putin's closest associate, Yevgeny Prigozhin, who is known as "Putin's chef" is behind brutal intimidation tactics against Russian bloggers and social media activists who are considered regime critics. According to the source, Prigozhin is the head of the "troll factory" in St. Petersburg, which is accused by the US investigation as the one behind the meddling in the 2016 US presidential elections. Apparently, the same Prigozhin is behind the series of assassinations of Russian bloggers and regime critics. Most of the assassinations were conducted using chemical poison. Prigozhin is also known as the head of Russian private military company "Vagner," which is actively engaged in Syrian fighting.

http://bit.ly/2CKxY6F

MIDDLE EAST

Naoris rollout blockchain-based cybersecurity in the Middle East

Naoris has been introduced to the Middle East after Sheikh Mohammed bin Rashid Al Maktoum launched the "Dubai Cyber Security Strategy" in 2017. Naoris, launched in 2018, is a holistic blockchain-based cybersecurity ecosystem, which offers a game-changing solution to address cybersecurity in rule-based systems. The IT solution company PROW is going to utilize Naoris' artificial intelligence and blockchain-based platform to protect their clients' networks. The current security systems work with multiple devices on the same network, which can, if hackers get access to the system, have huge consequences for the organizations. Naoris functions on a platform that allows detection and reporting of cyber threats but also spreads an organization's information over multiple servers and devices. In previous settings, a secure network of organizations in the became less secure as more devices were connected, but Naoris' solution becomes more secure as it expands.

https://bit.ly/2OTImiS

GCC shelling out 66 percent more than global average on every data breach

According to a study by the research company Gartner, Gulf Cooperation Council (GCC) nations spend 66 percent more on data breaches than the global average. The GCC nations are upping its investment in data protection after more than 300 cyberattacks were reported last year. Worldwide organizations and nations are spending $2.1 million on stopping data breaches, compared to $3.5 million typically spent in the GCC, according to Gartner, which is based in the United States. A principal research analyst at Gartner, Sam Olyaei, said "usually three to four security analysts are required

to detect such attacks in time but in this region there is an average of zero to one."

https://bit.ly/2OVH6wB

ASIA PACIFIC

Japan set to outsource some of its cyber defense operations

Japan's Defense Ministry is set to hire private cybersecurity experts by the end of the year, as part of its efforts to tackle cyber threats affecting critical infrastructure. The experts will join a team to up of 150 employees in 2018, increasing to 220 in 2019, and will be highly paid for their work, which was factored in the yearly defense budget. The experts will focus on monitoring and analyzing malware threats. Japan is focusing on cyber defense, and considering joining Locked Shields, an international cyber defense exercise, conducted by the Estonian- based NATO Cooperative Cyber Defense Center for Excellence.

https://goo.gl/GYG8p8

China's Huawei and Spain's National Cyber Security Institute (INCIBE) launch a cybersecurity competition

The Cyber Security Cyber Talent Challenge registration will be open from October 30 to November 18 and aims at young professionals in the cybersecurity field. This is part of the partnership between China's Huawei and Spain's INCIBE, which signed an agreement in 2016.

Director of INCIBE said that Spain is well prepared for cybersecurity threats but has a shortage of young professionals in the much-needed field. He added that this is part of an ongoing effort to create new jobs, and investments in new companies, for which Spain has allocated large amounts of funds. One of the emphases in their cooperation is promoting research and development.

https://goo.gl/XQGfpm

Singapore will set up the first International Risk Pool

The announcement was made by Singapore's finance minister, Heng Swee Keat, at the Singapore International Reinsurance Conference. The pool, which will commit to up to one billion dollars, will allow corporations in Asia to be protected against cyber-related losses. So far, twenty insurance firms have shown interest in joining. Mr. Heng said that at least 60 percent of Asian companies does not have comprehensive cyber threat monitoring tools. Insurance coverage of cyber threats is generally very low across the globe, due to a lack of historical data and intelligence. Mr. Heng announced also the opening of the Global Asia Insurance Partnership, which will incorporate global insurance industry, regulators, and academic research.

https://goo.gl/pz9YSo