Global Cyber Bi-Weekly Report by INSS May 15 2018

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

Contributors: Simon Tsipis, Ido Sivan, Anna Danilova, Sneha Mukherjee, Bryan McCarthy

ISRAEL

Shin Bet head: Big data prevents but also could escalate threats to Israel

The Shin Bet (Israel Security Agency) is at the forefront globally in using big data to prevent terrorist attacks, but its use also has escalated the threats posed by the nation's enemies, according to the agency's director, Nadav Argaman, in an article to be published late on Wednesday in the Israel Intelligence Heritage and Commemoration Center journal. "The world of big data and cyber confronts the intelligence community with more complex challenges than ever before," he writes, and adds that "looking forward, our enemies are not stagnant, as the world of big data develops and broadens and technology is becoming more advanced every minute." This challenge has led to a new conceptual approach with the Shin Bet defining the areas of technology and information as being "critical resources in intelligence collection and in prevention of the enemy's [plans]," he writes. The keys to the Shin Bet's success in preventing terrorist attacks in this new age are its spiked investment in agents with cyber expertise, new technologies, thoughtful coordination between its cyber and operational units and better coordination than ever before with other elements of Israeli intelligence. "These elements are also the keys which will preserve our achievements in the future and our continued ability to guarantee peace and security for the State of Israel," Argaman wrote.

https://bit.ly/2I2JApr

Israeli cybersecurity company Protego raises 2 million dollar

Israeli cybersecurity company Protego, with offices in Jerusalem and Baltimore, Maryland, has raised $2 million in seed funding led by Ron Gula of Gula Tech Adventures, Glilot Capital Partners, and the MetroSITE Group of security industry pioneers, including former RSA CTO, Tim Belcher. The company's CEO Tsion Gonen said, "Protego is the first and only platform of its kind that delivers full life-cycle

security to serverless applications from deployment to run-time - that can be up and running in just 20 minutes. With this investment, Protego will continue to work with customers and partners to broaden our offering and bring the product to market." According to Gula, serverless computing represents a transformative step in leveraging the full potential of the cloud, but it will require enterprises to think and act differently about application security .

https://bit.ly/2rEcdz1

UNITED STATES

Without a nuclear deal, United States expects resurgence in Iranian cyberattacks

The United States and Israel are expecting renewed cyber operations by Iran since President Trump's announcement of withdrawing from the JCPOA. Unit 8200 and the National Security Advisory (NSA) have already noticed a surge in Iranian cyber operations targeting US military bases in Europe as well as foreign ministries of US allied nations. According to experts and intelligence officials, the consensus is that Iran now has nothing left to lose and will therefore target the United States and Israel more vigorously. It is also noted that since Israel's air strike on fifty mostly Iranian targets in Syria, Iran will have a more immediate score to settle with Israel.

https://nyti.ms/2KWyQab

Cybercom to elevate to combatant command

The US Department of Defense announced that the US Cyber Command was elevated to a combatant command on May 4. This makes the Cybercom one of ten combatant commands. As Pentagon spokeswoman Dana White said, "The cyber domain will define the next century of warfare . . . Just as our military must be prepared to defend our nation against hostile acts from land, air, and sea, we must also be prepared to deter, and if necessary, respond to hostile acts in cyberspace".

https://bit.ly/2JVdlVU

Senate confirms Paul Nakasone to lead the NSA, US Cyber Command

Army Lt Gen Paul Nakasone will be receiving his fourth star and command of the NSA as well as of the US Cyber Command. He replaces Admiral Mike Rogers who is retiring after thirty-seven years in service. General Nakasone will be tasked with deciding rather soon if his position can effectively command both the NSA and Cybercom or if the two need to be separated and command positions established for both.

https://wapo.st/2rGTpyt

EUROPE

World's first advanced blockchain identity lab to be built in Edinburgh

An international collaboration has been announced in building the "world's first" advanced blockchain identity research facility in Edinburgh. The laboratory will be built at Edinburgh Napier University's Merchiston campus as part of a £600,000 partnership between the university and the Hong Kong-based Blockpass. Blockpass is currently using blockchain technology—a growing list of records or blocks secured using cryptography—to develop an identity verification platform.

https://bit.ly/2IcxH0d

UK manufacturers are top attack target for cybercriminals

Manufacturing was the sector most attacked by cybercriminals in the United Kingdom last year, a report from NTT Security has found, mirroring warnings from other agencies, including the UK's National Cyber Security Center (NCSC). The firm's Global Threat Intelligence Report 2018 found that finance was the most targeted sector worldwide, accounting for 26 percent of attacks, including ransomware, phishing denial-of-service, and other techniques. The same study also found that ransomware infections grew by 350 percent from last year.

https://bit.ly/2IcMNCY

Europe's new data protection law: what will change?

The European Union's General Data Protection Regulation (GDPR) is the biggest overhaul of data privacy laws in over twenty years. The law will come into force on May 25, giving EU citizens new rights over how their personal data are used. Companies doing business in the European Union will face new rules about how they handle people's data and stiff penalties for breaching the law.

https://reut.rs/2GbgEGd

A quarter of UK infrastructure organizations have suffered cyberattack outages

Over a third of critical infrastructure outages in the United Kingdom over the past year were due to cyberattacks, according to a new Freedom of Information request. Corero Network Security received responses from over 200 critical infrastructure organizations, including fire and rescue services, police forces, ambulance trusts, NHS trusts, energy companies, water authorities, and transportation bodies. It found that 70 percent had suffered a service outage over the past two years, with 35 percent of these disruptions the result of cyberattacks.

https://bit.ly/2rLgwIj

RUSSIA

A Russian breakthrough? Optical fibers to be used in creating lasers

Physicists from the Russian Academy of Sciences have developed a new type of optical fiber, which can be used as a base material for creating bright and compact infrared lasers. In recent years, as reported by Firstov and his colleagues, engineers have begun to use fiber optic not only to transmit information but also as a working fluid for so-called fiber lasers.

http://bit.ly/2IBomys

Putin transfers all government and social infrastructure to Russian-made software

President of the Russian Federation, Vladimir Putin, instructed the Russian government to transfer all government agencies and institutes to Russian-made software infrastructure until 2024. According to the decree, the government should ensure "the use of predominantly domestic software by government agencies, local governments, and organizations." As follows from the decree, the government needs to ensure information security based on domestic developments in the transfer, processing, and storage of data that guarantees protection of the interests of the individual, business, and the state.

http://bit.ly/2GbNnuW

The website of the Civil Aviation Agency of ex-soviet Georgia subjected to cyberattack

On May 2, unknown persons committed a cyberattack on the server of the Civil Aviation Agency of the Georgian Ministry of Economy and Sustainable Development (GCAA), which damaged programs and blocked a protected database. According to the deputy head of the agency, Levan Kanadze, hackers may have been seeking financial goals and intended to demand a ransom for unlocking the database.

http://bit.ly/2jQKAyq

MIDDLE EAST

Without the nuclear deal, Iranian cyberattacks resume

Government and private-sector cybersecurity experts in the United States and Israel worry that US President Trump's decision to pull out of the Iran nuclear deal this week will lead to a surge in retaliatory cyberattacks from Iran. Within twenty-four hours of Trump's announcement that the United States would leave the deal, researchers at the security firm CrowdStrike warned customers that they had seen a "notable" shift in Iranian cyber activity. Iranian hackers were sending emails containing malware to diplomats who work in the foreign affairs offices of US allies and employees at telecommunications companies, trying to infiltrate their computer systems.

https://bit.ly/2wF5Lgc

More than a million online shoppers in UAE exposed to scams

The rapid rise of e-commerce in the United Arab Emirates has exposed more than a million online consumers to shopping scams, according to a report by security experts at Norton. A 2017 cybersecurity insights report revealed UAE shoppers lost more than $90 million, with a quarter of victims having their financial details compromised as a result. Norton research found 90 percent of UAE consumers now shop via mobile devices despite 71 percent of respondents surveyed admitting that the trend was risky.

https://bit.ly/2K9hLIv

Islamic State's media outlet silenced but not for long

The cyber divisions of law enforcement agencies in the United States and seven other countries launched a massive operation last Thursday to disrupt the Islamic State's "capability to broadcast terrorist material for an undetermined period of time." A primary target was the online media portal, Amaq. Amaq did disappear from the internet on Thursday, the day before the coordinated operation was publicized by the pan-European police agency, Europol. But by Wednesday morning, Amaq was back online, seemingly hosted on a server in Phoenix, Arizona.

https://cbsn.ws/2rlcAOR

CHINA and APAC

Facebook launches email-based hotline for data security of Indian politicians

To prevent Indian politicians and their political parties from cyberattacks, the social networking giant Facebook has launched "Cyber Threat Crisis," in which it will provide an email-based hotline to India's politicians and political parties in order to secure their data. With the hotline, compromised accounts and even the Computer Emergency Response Team (CERT-IN), which works under union ministry of electronics and IT, can write to indiacyberthreats@fb.com in the event of cyber interference, including suspected hacks. Facebook also released a "cyber hygiene guide" for political accounts. These include best practices for politicians and political parties on how to secure their Facebook pages and accounts.

https://bit.ly/2rFxSXA

China-developed cyber mimic defense withstands 500,000 attacks

A cyberspace security system based on the China-proposed mimic defense theory has withstood over 500,000 hacker attacks in an international challenge held in Nanjing, the capital of eastern China's Jiangsu Province The mimic defense system features an ever-changing software environment, which makes conventional hacker attacks difficult to locate a target. The system is expected to change the current "ex post facto defense" pattern in cybersecurity, according to Wu Jiangxing, the academician who first proposed the theory.

https://bit.ly/2IE95wU

How can Japan-UK cybersecurity cooperation help ASEAN build cybersecurity capacity?

Southeast Asia is a lucrative market for tech investment, and the United Kingdom wants access to it. Japan can help. Japan and the United Kingdom held their fourth bilateral dialogue on cyberspace in London to discuss their cooperation on the Tokyo Summer Olympic and Paralympic Games, the development of international cyber norms, the security of the Internet of Things devices, and capacity building. Southeast Asia is a lucrative market for tech investment as the region becomes more connected to the internet. The region received $274 billion in foreign direct investment last year, and that number is poised to grow thanks to investments from Japan, China, and India. The region is also the fastest growing internet market in the world, adding 3.8 million internet users every month. The region's digital economy was worth $31 billion in 2015, and is expected to grow to $197 billion by 2025. If Japan can learn from the United Kingdom, then what is in it for London? The answer is simple: access to the Southeast Asian cybersecurity market via capacity building efforts.

https://on.cfr.org/2ERTgN6