Global Cyber Bi-Weekly Report by INSS January 15 2018

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

Contributors: Simon Tsipis, Ido Sivan, Matan Tomer, Sanjana Rathi, Anna Danilova

ISRAEL

Israel's IAI, Poalim Bank to create cyber solutions using Blockchain technology

Israel's largest bank Poalim Bank and prime aerospace and aviation manufacturer Israel Aerospace Industries (IAI) have announced collaboration for leveraging Blockchain technology to create innovative cyber solutions. The joint research undertaken by the two companies will examine how Blockchain, the innovative technology at the basis of cryptocurrencies such as Bitcoin, could be used for developing innovative cybersecurity solutions, such as secure transmission of information between services and supply chains, user authentication, critical devices and elements that run with no human intervention, and additional solutions for the cyber challenges in a hyper-connected world.

http://bit.ly/2FBDPdy

Igal Unna named new cyber chief

Prime Minister Netanyahu has named Yigal Unna as his choice for heading the National Cyber Security Authority. Unna, previously headed the Israel Security Agency's Cyber and Technology division from 2014–2017 and was also a longtime veteran of the IDF's Unit 8200, "Israel's NSA."

http://bit.ly/2FAu0wj

UNITED STATES

FBI chief: Encryption is "urgent public safety issue"

During a speech at the International Conference on Cyber Security in New York, the FBI Director, Christopher Wray, stated that the inability of law enforcement agencies to surpass the strong encryptions on electronic devices poses an "urgent public safety issue. While the FBI and law enforcement happen to be on the front lines of this problem, this is an urgent public safety issue for all of us," said Wray. In the last fiscal year, the FBI failed to break through the powerful protective coding of 7,775 devices, even though they had advanced tools at their disposal and the legal right to access the contents.

https://goo.gl/qfPf57

House passes NSA spying bill after Trump tweets cause confusion

The US House of Representatives passed a bill to renew the National Security Agency's warrantless internet surveillance program, overcoming objections from privacy advocates and confusion prompted by tweets from President Donald Trump who initially questioned the spying tool. The vote was a major blow to privacy and civil liberties advocates, who just two years ago celebrated the passage of a law effectively ending the NSA's bulk collection of US phone call records, another top-secret program exposed by Snowden. The bill passed by the House would extend the NSA's spying program for six years with minimal changes. Some privacy groups said it would actually expand the NSA's surveillance powers. Most lawmakers expect it to become law, although it still would require senate approval and President Trump's signature.

https://goo.gl/DFa3Ht

EUROPE

UK: Data protection bill amended to protect security researchers

Exemption added after researchers said efforts to demonstrate inadequate anonymization could fall foul of law. The government is to amend the data protection bill to protect security researchers who work to uncover abuses of personal data, quelling fears that the bill could accidentally criminalize legitimate research. The bill will contain a clause making it a criminal offense to "intentionally or recklessly re-identify individuals from anonymized or pseudonymized data," with the potential of an unlimited fine for offenders.

http://bit.ly/2CZjJbg

Der Spiegel: German cyber agency calls for authority to hack back

Germany spy agencies should have the authority to digitally strike back against cybercriminals, the president of Germany's new cyber security agency Zitis told Der Spiegel news magazine.

"As a citizen I expect that our government remains able to act even in the face of new digital threats," Wilfried Karl was quoted as saying in an interview. Zitis was set up earlier this year to help develop information technology (IT) tools to fight cybercrime and track the communications of potential terrorists. Karl made his comments a month after top German intelligence officials urged lawmakers to give them greater legal authority to "hack back" in the event of cyberattacks from foreign powers.

http://bit.ly/2myXFOF

France might vet acquisitions of artificial intelligence, data protection firms

The finance minister says France may add artificial intelligence and data security to a list of nation's strategically important, regulated sectors. This move could enable the government to block foreign takeovers of French companies in those industries, Finance Minister Bruno Le Maire said. As Reuters reports, a decree made in 2014

already requires foreign companies to get permission from the French state before taking control of firms in the energy, telecoms, transport, water, and health sectors.
http://ubm.io/2FA4J5E

Finnish police start investigations over forest company hacking

Finland's National Bureau of Investigation (NBI) said it would start investigations on a suspected data breach at Metsa Group, one of the Nordic country's largest forest companies. Metsa Group and its listed subsidiary Metsa Board on Tuesday released preliminary results due to suspected hacking but gave no further comments about the breach or actions taken. The NBI said it was investigating the case as a serious computer break-in. Metsa Group had sales of around 4.7 billion euros ($5.6 billion) in 2016.
http://reut.rs/2AVDj6A

RUSSIA

Opinion: Russia might outrun the west in military technology race

The United States risks losing to Russia in technological development due to robotics and artificial intelligence developments, according to CNN commentator Zachary Cohen. The journalist remembered the words of Russian president Vladimir Putin, who said that the world leadership will be in hands of a country that will outstrip others in developing artificial intelligence. The observer also noted that the Russian army is developing robots, drones, destruction systems, and cruise missiles that could analyze radar data and independently solve and decide what kind of speed or height to take and in which direction to fly.
http://bit.ly/2BG3dRa

Kaspersky Lab tries to minimize the damage due to suspicions of its Russian government linkage

Kaspersky Lab said that it is discussing with the British Center for National Cybersecurity (NCSC) the creation of an independent verification mechanism for the

security of its products and services. Earlier, the Financial Times reported that NCSC head Kiaran Martin had warned the national security agencies of the risks of using Kaspersky Lab software.

http://bit.ly/2pla0da

Federal Security Service's cyber authority expanded by Russian president

Russia's President Vladimir Putin signed the decree "On Improving the State System for Detecting, Preventing and Eliminating the Consequences of Computer Attacks on Information Resources of the Russian Federation." According to the decree, the Federal Security Service (FSB) is responsible from now on for detecting, preventing, and eliminating the consequences of computer attacks on Russia's information resources.

http://bit.ly/2BoHOHR

High probability that Chinese hackers are attacking Russian military RD facilities

Security experts from Kaspersky Lab published a report on attacks using malware Travle, also known as PYLOT. The attacks are mainly aimed at government organizations, the armed forces, the development of weapons, and hi-tech located in Russia and CIS countries. Malicious software is distributed through fishing emails disguised as materials about the joint Belarusian-Russian military exercises "West-2017." The attackers are presumably Chinese-speaking, the experts noted.

http://bit.ly/2BTaFVH

MIDDLE EAST

Internet cut-off during recent unrest in Iran reveals state's cyber capabilities

Iran's efforts to control the internet were realized during recent disruptions when the regime was able to block major social media outlets used by the protesters. A seventy-six-page report by the Center for Human Rights in Iran details Tehran's new

capabilities to monitor and block online communications. Some of the exposed capabilities include the ability to separate domestic from international internet traffic, identify users, hack into private accounts, filter online content in search engines, and violate net neutrality principles to make local services faster and cheaper than the global ones.

http://bit.ly/2D9rUWJ

Social media battles between the Iranian government and protesters

The streets are not the only battleground between Iran and its critics. A cyber battle on several fronts is being fought between the two sides on social media platforms. As opposed to the 2009 protests, today's messaging apps are used by higher percentage of the population, and the government is better prepared to confront its opponents in the digital media as well. In the absence of independent news outlets and state television's typically one-sided coverage, citizens have taken to social media to share photos and videos of the demonstrations with the aim of disseminating their message and inviting more local residents to join the crowds. Telegram—which has an estimated forty million users in Iran, equivalent to almost half the population—has been the platform of choice for the protesters. In response, the officials have "temporarily" blocked Telegram and Instagram. Facebook, YouTube, and Twitter have been banned since 2009. Further, one of the notable tactics used was the creation of dozens of Twitter bots whose job ranged from claiming that widely shared videos of rallies are fake, to discouraging potential protesters from joining rallies.

http://bbc.in/2m3Nr85

Fortinet experts argues UAE is well positioned to face cyberattacks

Compared to the rest of the Middle East, the UAE is well positioned to counter cyber threats, according to an expert at the network security firm Fortinet. "There is a lot more awareness regarding security and they are closer to the top of the curve of uptake of digital solutions. The UAE also has cybersecurity legislation in place, which is a big positive," said Simon Bryden, consulting system engineer in Fortinet. The

adoption of new technologies differs from country to country, but from the perspective of the Gulf countries, the UAE has always been ahead in adopting new technologies, said Patrice Perche, senior executive vice-president for worldwide sales and support at Fortinet. "In this regard the country exhibits the same dynamics as seen in South Korea and Singapore," he added.

http://bit.ly/2CMpi00

CHINA and APAC

How safe is digital India?

Recently India witnessed a massive drive by the government and India Inc to link tax returns, bank accounts, mobile SIMs, mutual funds, and more to the twelve-digit Aadhaar Biometric. Many data leaks incidents with Aadhaar raises many questions about India's digital security. To reassure that 1.19 billion Aadhaar users' details are not accessible over platforms like WhatsApp, the Unique Identification Authority of India provided an option to create a sixteen-digit virtual ID to mask the real Aadhaar. According to Saket Modi, CEO of Lucideus, no bank account has been compromised because of Aadhaar's data leaks, because a majority of the non-biometric information that Aadhaar captures is already in the public domain and people also share more voluntarily on Facebook and other social media platforms. However, according to Akhilesh Tuteja, despite an unbreakable 2048-bit encryption, anything can be hacked. Also, the concerning factor that only 1–3 percent of the IT budget is allocated to cybersecurity has been highlighted, with the fact that in September 2017, the Ministry of Electronics and IT mandated all government departments to spend 10% of their technology budget on security.

http://bit.ly/2mtxbxn

Israeli firm planning security academy in Gujarat

An Israel-based security firm is planning to set up an academy to impart training in the state. A high-level delegation from Israel visited Gujarat Chamber of Commerce and Industries on Thursday to explore business and collaboration opportunities in

the state. Giving details about the plans, Tal Skornik, the managing director, said that every country has various levels of security needs and strengthening security systems helps to ensure normality in operations, be it business or a country's administration. The firm plans to provide courses in officer security, general security, VIP protection, port security, airport security, cyber security, and technology security.

http://bit.ly/2AXSpby

Regulator probes Marriott for violating China's cybersecurity law following Tibet incident

A call for investigation has been made after the global hotel chain Marriott International allegedly listed the Tibet Autonomous Region of China as a country in an email, after a Twitter account affiliated with the Marriott "liked" a "post-independence of Tibet" tweet. According to Shanghai Police, this conduct is a violation of China's law on cyber security and advertisements. The regulators have asked the company to withdraw the content in question and to conduct an overall check on information released online and on its apps.

http://bit.ly/2DgcVJV

Japan's prime minister gains cybersecurity support in meeting with Estonian counterpart

A bilateral agreement on cooperation in cybersecurity was signed between Japan and Estonia, allowing Tokyo to take advantage of Estonia's expertise, and to strengthen economic ties with Estonia. It was also asserted in Prime Minister Abe's visit to Estonia that Japan will soon become a contributing participant in the NATO Cooperative Cyber Defense Center of Excellence, located in Tallinn.

http://bit.ly/2mAYzKx