Global Cyber Bi-Weekly Report by INSS Mars 01 2019

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

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

ISRAEL

Cyberattack reveals worrying flaws in Israeli online security

As many as one million Israeli websites, including those of major banks and telecom companies, were hacked over the weekend. The websites in question were only offline for a short period of time, replaced with text reading "Jerusalem is the capital of Palestine #OpJerusalem."

https://bit.ly/2VCO4Wm

Israeli cyber hotline offers help for the hacked

Staffed mostly by veterans of IDF computing units, the world's first emergency response center for victims of cyberattacks opened its doors in the southern high-tech hub city of Beer Sheva.

It enables businesses and private individuals to report suspected hacking and receive real-time solutions. The 119 call-in number to the Computer Emergency Response Center (CERT) is being billed by Israel and cyber experts as a world first. "Our job is to mitigate the damage as quickly as possible, to learn about the threats and to spread the knowledge where relevant," CERT director Lavy Shtokhamer told Reuters.

https://bit.ly/2UhAIhK

German army seeks to partner with Israeli cyber and artificial intelligence startups

The German army plans to start working with Israeli companies and expand cooperation with Israeli startups, Marcel "Otto" Yon, CEO of the Bundeswehr Cyber Innovation Hub, the digital innovation unit of the German Armed Forces, said at Calcalist's WeTechBerlin conference. "We want to look at the

Israeli market more systematically," he said. Investing in Israeli companies and startups is part of the innovation hub's mandate to expand globally, Yon said. Representatives of the Bundeswehr Cyber Innovation Hub visit Israel regularly and meet with their counterparts in the Israeli military and commercial startup accelerators, according to Yon.

https://bit.ly/2Ce6pll

UNITED STATES

Deadline passes for companies to comply with New York's cybersecurity regulation

New York, a major hub for global banking and finance, has endured the consequences and growing threat that illicit actors and activity poses to sensitive data and financial systems. Subsequently, two years ago, the New York State Department of Financial Services Cybersecurity Regulation (23 NYCRR Part 500) was declared and went into full effect on the first March. The substantial number of rules and possible penalties are designed to ensure certain standards are met by a larger amount of financial services companies. "Covered Entities" include banks, mortgage brokers, insurers, charities, third party companies, international subsidiaries operating in New York, and other entities that vary in the number of provisions with which they are required to comply. Exemption is based on revenue, number of New York employees, control of either or both information systems, and nonpublic information, to name a few; as such, compliance varies among companies and organizations. Nonetheless, covered entities have a seventy-two-hour breach notification condition, similar to the EU General Data Protection Regulation. Other requirements, relevant to certain provisions, warrant the use of "encryption, multi-factor authentication, third party risk assessments, penetration tests, and audit trails." The department has also inquired with Facebook and mobile app developers regarding the use of data without user consent.

https://bit.ly/2Et8kTo

Insider-threat competition releases a cyber wolf in its flock

Most recently, US Cyber Command demonstrated its public-private partnership initiative, with an insider-threat detection competition, run by the Maryland Innovation and Security Institute at the DreamPort facility. "Wolf in

Sheep's Clothing" occurred during January and February, entailing contributors to create, implement, or improve "user activity monitoring solutions to detect live and recent insider-threat attacks, as well as unauthorized activity." Albeit the current available solutions, the central attention was for solutions that provide "predictive monitoring features." DreamPort set up Windows and Linux machines, using human actors to interact in real-time. Jazz Networks placed first, with the solution that detected all the unauthorized actors and activities.

https://bit.ly/2GULpDX

EUROPE

Brussels teeming with Russian and Chinese spies, EU officials claim

"Hundreds" of Russian and Chinese spies have been planted in and around Brussels' EU quarter, according to officials at the European External Action Service (EEAS). There are currently "about 250 Chinese and 200 Russian spies in the European capital," the German newspaper, Welt am Sonntag, reported over the weekend, citing diplomats at the EEAS, the EU's foreign policy office. The officials revealed they have been warned about spending time in certain premises around the EU district, including popular restaurants and cafés in the vicinity of the European Commission's Berlaymont building.

https://bit.ly/2ByBfVa

European Commission urges recall of children's smartwatch

If you have been on a trip to Germany recently and picked up a few gifts for the family, you might want to take note if you happened to buy the Enox Safe-KID-One smartwatch for children. Despite "safe" appearing in the watch's name, it is actually anything but safe. In fact, the European Commission has gone as far as to urge distributors to recall every single watch from anyone who purchased it because it is a "serious risk." Enox Group, the company behind the Safe-KID-One, describes the smartwatch as a high-tech GPS safety and surveillance watch that helps parents keep track of their children and enable them to talk to their children all the time.

https://bit.ly/2N4CfVN

Europe hopes to fend off election hackers with "cyber sanctions"

A regime for "cyber sanctions" is taking shape, and it could already hit mischievous election hackers in May. The European Union is closing in on a procedure that would allow it to sanction foreign hacker groups when they target the upcoming EU election. A plan drafted by the European Union's diplomatic service has been presented to national cyber experts and will be forwarded to foreign affairs attachés later this month, three officials briefed on the plan told POLITICO, asking not to be named because of the sensitivity of the ongoing talks.

https://politi.co/2Iii5Jg

United States warns EU allies not to use Chinese gear for 5G networks

The United States sees the European Union as its top priority in a global effort to convince allies not to buy Huawei equipment for next-generation mobile networks, a US State Department Official said in February. After meetings with the European Commission and the Belgian government in Brussels, US officials are set to take a message to other European capitals that the world's biggest telecommunications gear maker poses a security risk, said the official, who declined to be named. "We are saying you need to be very, very cautious and we are urging folks not to rush ahead and sign contracts with untrusted suppliers from countries like China," the official said.

https://bit.ly/2STNoy2

RUSSIA

US intelligence: Russia is already capable of massively cyber-striking the United States

After Russian media source Svoboda became familiar with the US Intelligence assessment of the most acute security threats, it released an article noting that the Russian cyber threat, along with the Chinese, are considered the most dangerous threats, even more than international terrorism. Russian operations in cyberspace have attracted more attention because they have threatened the US presidential elections, and they represent a long-term strategic threat

to the United States, as stated in the US intelligence assessment. According to the assessment, Russia is interested in influencing the American public opinion and is preparing for cyberspace battles. US intelligence had made a sensational conclusion that Russian hackers have implemented virus programs in the systems that control power lines in the United States, and they are supposedly already able to interrupt the flow of electricity in the United States for several hours. The assessment concludes, that Russia today is already capable of striking the United States without using any military or weapon systems.

http://bit.ly/2WYTZpT

Ex-commander of US Cyber Command: Less words, more deeds against Russia

Retired Admiral Mike Rogers, who until recently served as director of the National Security Agency and commander of the US Cyber Command, said that to effectively cyber-deter Russia, the United States must move from rhetoric to action. According to Rogers, publicly acknowledging our cyber capabilities and that we use them, as we did when comparing our cyber capabilities against ISIS in 2016, is essential in deterring Russia's cyber aggression. In addition, US lawmakers must loosen some restraints on the military's use of cyber weapons, Rogers said.

https://cbsn.ws/2Bzt1MD

US intelligence community's report: Putin directly ordered the attacks

In a report prepared and released by the CIA, FBI, and NSA, the US intelligence community states that all major cyberattacks of US government institutions and processes were ordered directly by Putin himself. Russia's intelligence services, the report confirmed, conducted cyberattacks that targeted "both major US political parties." The report confirmed that the GRU, Russia's military intelligence service, was behind the attacks and used Guccifer 2.0 and dcleaks.com to publicly release US victim data, and it also relayed material it acquired from the Democratic National Committee and senior Democratic officials to WikiLeaks.

https://cbsn.ws/2BrKSoL

Russia is about to disconnect itself from the World Wide Web

The Russian government supported a bill about the possibility of isolating Russia from the global network, according to TASS reports. The bill was submitted to the State Duma in December 2018, and among its authors were Head of the Federation Council Committee Andrei Klishas and State Duma Deputy Andrei Lugovoi. The authors argue that adopting the bill is necessary, particularly given the threats of aggressive actions in cyberspace, allegedly emanating from the United States. Disconnection from the global network to protect against threats, according to the authors of the bill, should ensure the "sustainability" of Russia's internet. It should be noted that Duma Deputy Andrei Lugovoi is an ex-FSB, Russian Security Service agent, who was accused by the British Government in the deadly poisoning in 2006 of Alexander Litvinenko, a former officer of the Russian FSB secret service, who had defected to Britain.

http://bit.ly/2Srn7HU

Russia is about to spend billions on disconnecting from the global internet

20 billion rubles will be spent on implementing the draft law for creating an autonomous internet in Russia, as announced by the author of the bill, Andrei Klishas. It was reported that in 2019, approximately 600 million will be spent on creating a monitoring and control system for the "Russian public telecommunications network." Approximately the same amount is planned to be spent in 2020 and 2021 on the "subsequent implementation of the project," the agency's source said.

http://bit.ly/2BycOHz

MIDDLE EAST

Cybersecurity firm Resecurity links a 2017 attack on the UK Parliament with hacking of the Australian Parliament

Iranian-backed hackers who stole personal data from Australian lawmakers earlier this year are the same group that attacked the British Parliament in 2017. New research by the Los Angeles-based Resecurity sheds light on Iran's campaign of cyberespionage against its adversaries. The hack of the

Australian Parliament "is a part of a multi-year cyberespionage campaign" by an Iranian-backed hacking group called "Iridium." "This actor targets sensitive government, diplomatic and military resources" in Australia, Canada, New Zealand, the United Kingdom, and the United States, the firm says. Although Australia has not formally attributed the attack to Iran, the Wall Street Journal first reported on the Iranian connection this month.

https://nbcnews.to/2UedVDE

CCQ prepares for graduation of Qatar's first batch of cybersecurity experts

The Community College of Qatar (CCQ) is currently preparing for the graduation of the country's first batch of students with a bachelor's degree in Cyber and Network Security. The graduates will play a leading role in protecting the nationwide information and communications technology (ICT) infrastructure that will help facilitate Qatar's anticipated socioeconomic transformation. This program will answer to the increasing demand for highly-trained cybersecurity professionals in the run-up to 2030 and the establishment of a knowledge-based society. Having placed ICT development at the top of its priorities, the government of Qatar has taken steps to build a smart digital infrastructure that can help achieve the objectives of the country's national vision, by powering its augmented healthcare services, technology-assisted learning environments, modernized business models, and environmentally sound technologies, among other enhanced outcomes. CCQ president Dr Mohamed al-Naemi stressed that the sheer volume of data transmitted through such a massive interconnected network requires coordinated efforts in order to protect and secure.

https://bit.ly/2TsFWdr

APAC

Australia's parliament hack: Iran or China still main suspects

Earlier in February, the Australian government revealed that all Australian political parties were targeted in a hack by a "sophisticated state actor" in a breach of security, which revealed that thousands of parliament members' email addresses and personal details were possibly stolen. Resecurity, an American security firm, linked the attack to Iran's Mabna Institute hackers, as

reported in the Wall Street Journal, claiming that it was part of a global espionage campaign, targeting the Five Eyes Alliance: United States, Canada, United Kingdom, Australia, and New Zealand. Resecurity's director, Charles Yoo, provided as evidence a database of 7,354 records containing phone contacts and emails for Australian parliament members and staffers. However, Australian sources with knowledge of the hack dismissed Iran's Mabna group as the primary suspect and point its fingers at China, without providing concrete evidence. They said that the government blocked the hacking attempt before learning the identity of the attacker. China has been behind previous cyberattacks on Australian government systems, including a 2011 hacking of the federal parliamentary email network and the 2015 hacking of the Bureau of Meteorology. The hack occurred three months before national elections and raises concerns among government officials and public.

https://goo.gl/K1A1EM

Thailand passes law on cybersecurity

Thailand's military-run parliament unanimously has approved the Cyber Security Act. The law allows the National Cyber Security committee to summon individuals for questioning, enter private property without court order, and, in case of cyber security event, will allow the government to override all procedures with its own law. Internet freedom activists claim this law, among others, which are used to crack down on dissidents, acts as a "cyber martial law" and ignore rules of privacy. Civil liberty advocates, businesses, and internet companies protested against the law, claiming it overrides the rule of law, and privacy act laws. It might also drive foreign investors and businesses out of Thailand. The army, should it activate the law in a "critical emergency," will not require a court order, and criminal charges will be leveled against those who fail to comply.

https://goo.gl/ExqAYx

Japan and India to work together on combating cyberattacks against 5G Technology

In the third round of bilateral talks in Tokyo, Japan and India discussed cooperation on cyber risks related to 5G technology, mainly from products of Chinese telecommunications giant Huawei. The agreement will focus on sharing information regarding illegal access of data and preventing

dominance of Chinese products in the fast growing Indian market. India is on a fast path to becoming an economic world power. As such, China aims to penetrate the growing 5G market there as part of its "belt and road" economic initiative. Japan has already adopted a new policy of excluding Huawei and ZTE products. The meeting between Japan and India, in part, is an attempt to join forces against China. Japan places high importance on its relations with India as part of the "free and open" Indo Pacific initiative. In a summit meeting in October 2018, Japan and India agreed to promote joint research on AI and strengthen security ties. If India's communications network could potentially be illegally breached, it will pose a risk to joint projects.

https://goo.gl/pX2va7