Global Cyber Bi-Weekly Report by INSS March 1, 2020

Editor-in-chief: Gabi Siboni, **Editors:** Gal Perl Finkel, Gal Sapir
Contributors: Yael Elharar, Simon Tsipis, Rachele Buffa, David Murcia Briceño

ISRAEL

Instead of corruption: A division in the Comptroller's Office will focus on cyber

The Division for Special Offices in the State Comptroller's Office, which has been dealing with public corruption for fifteen years, will focus from the coming year on cyber audit and information systems. According to the auditor, technological changes and the increasing use of digital databases require the establishment of a professional and skilled wing to make sure that computing systems are well protected and there is no fear of a cyberattack. Matanyahu Englman rejected criticism that he decided to stop fighting corruption. The cyber audit and information systems emphasize the field of information security in order to ensure that government ministries and public bodies in Israel are prepared and ready for cyberattacks and to prevent the leakage of sensitive information to unauthorized parties. Therefore, it is of great importance to establish a skilled and professional department in the State Comptroller's Office, which can alert cyber deficiencies in advance and provide ways of improving the activities of the regulated bodies in this area.
http://tiny.cc/z0fukz

Netanyahu and Gantz's video war

After Netanyahu posted an edited video in which Gantz says "no women at the Blue and White polls," the Blue and White chairman uploaded a video to Instagram showing the Likud chairman stuttering as he tried to appeal to the Druze community. Netanyahu was fined NIS 7,500 by the Election Commission and was required to remove the video. The Blue and White party claim the

video they posted is authentic. On the afternoon of the election day, Prime Minister Benjamin Netanyahu posted on his Facebook page a video in which his rival, Benny Gantz, appeared to urge citizens not to vote for the Blue and White party that he heads. Gantz, for his part, posted a video on Instagram showing Netanyahu stammering as he tried to film a video intended for the Druze community. Although Facebook prohibits the posting of fabricated videos created using Deep Pike technology, it does not remove videos made by simpler means. Facebook responded, saying "We received an order from the Election Commission to block a video on the PM's page, but when we went to find the content to honor the court's order and restrict the content, we found that it was no longer on the platform."
http://tiny.cc/6kfukz

Israel's Toka advising Nigeria on cybersecurity

The Israeli company was selected by the World Bank for the project to enhance Nigeria's cyber development and to bolster the African country's national cyber resilience. The consultation will include working with government and institutional clients and will focus on the technical capabilities required in the field of information security and all that is needed to build capabilities and skills in the field. As part of the consultancy, Toka will assist in formulating best practices and will provide strategic recommendations in the field of cyber in terms of technical and operational implementation, as well as the construction of short and medium-term capabilities. Funding for the project will be made from World Bank funds supporting the Nigerian government to strengthen its cybersecurity.
http://tiny.cc/s5bukz

"Iran broke into hundreds of computers in Israel"

The cyber defense company ClearSky first revealed that Iranian hackers, operating under the auspices of the Iranian government, have broken into hundreds of computer systems in Israel and other countries, including government and security organizations and companies in the fields of

computers, telecommunications, energy, and aviation. According to the report, they were able to extract large amounts of intelligence information related to security projects and individuals. According to ClearSky's CEO, "we see Iranians improve their capabilities, [but] they can't get closer to nuclear information." According to the company's report, the Iranian attack campaign known as Fox Kitten has been running for the past three years. This is the most comprehensive and ongoing Iranian campaign to date. The intrusion into the mentioned computing systems was done by exploiting weaknesses in VPN access security systems, before companies were able to fix the loopholes.
http://tiny.cc/zmdukz

UNITED STATES

Cyber National Guard Task force will focus on network defense

In a recent ceremony, the US Army welcomed new units into the Army Cyber Command task force, according to press releases from the Department of Defense (DoD). Since its creation three years ago, over 450 Army National Guard soldiers have been assigned to the task force. Details are limited, but Task Force Echo, which falls under the Army Cyber Command and supports its mission more broadly, will likely work in network defense. The National Guard is considered a critical resource for the DoD's cyber work, considering that many personnel serve as cyber or IT professionals in their day jobs.
http://tiny.cc/r7jpkz

How the executive branch shaped the Cyber Solarium Commission

The Cyber Solarium Commission's report is due for release on March 11. The commission will release 75 cyber policy recommendations on a broad range of topics, and the executive branch took an active role. Suzanne Spaulding, one of the commissioners, said at the recent RSA conference, that representatives of the executive branch showed up for nearly all the

commission meetings and helped guide much of the report. Members from both chambers of Congress also sat on the commission. Because of the work with members of Congress, the final report will include an annex with "pieces of legislation" that Congress can pass pertaining to cyber issues. According to Spaulding, the members were "very interested in making sure that that things would not just fall on somebody's desk, but actually be achieved."
http://tiny.cc/7vjpkz

Cyber is the most "consequential" issue for Transportation Command

While the broader commercial defense logistics enterprise has improved its cyber hygiene, cybersecurity remains a critical concern for US Transportation Command. "The way I would characterize the cyber vulnerabilities is it's probably the most consequential to the mobility enterprise," Gen. Stephen Lyons, commander of the US Transportation Command, told the Senate Armed Services Committee recently. Given the heavy reliance on hundreds of commercial companies to move people and resources across the globe, cyber has long been a major concern for the leaders of the Transportation Command. Department of Defense leaders have become increasingly concerned that adversaries are targeting the defense industrial base for critical information. Lyons noted that these companies cannot withstand attacks from so-called advanced persistent threats. As a result, Transportation Command has built resiliency into its contracts.
http://tiny.cc/fujpkz

New Wi-Fi chip bug affects everything from Amazon's Echo to home routers

A large amount of internet-of things (IoT) devices are affected by a new vulnerability that could let a criminal or spy decrypt data sent over wireless connections. The flaw in widely used Wi-Fi chips made by Broadcom and Cypress essentially disables the encryption key used to secure

communications over popular wireless standards. Everything from certain classes of the iPhone to Amazon's Echo could be vulnerable to attacks tested by researchers at antivirus company ESET, who discovered the vulnerability, with the exception of two popular protocols, HTTPs and TLS. It is estimated that one billion devices are affected.
http://tiny.cc/xfkpkz

An FBI unit recovered $300 million of $3.5 billion in reported cybercrime losses last year

According to the Internet Crime Complaint Center (IC3), a unit inside the FBI that deals with cybercrime, $300 million was recovered of the roughly $3.5 billion in reported losses in 2019. The IC3 responded to more than 467,000 complaints in 2019, compared to 351,937 complaints in 2018. A person analyzes each complaint, who then determines whether to begin an investigation. According to the IC3 annual report, reported losses from ransomware attacks doubled in the past year to an estimated $8.9 million. Of the $3.5 billion reported stolen, an estimated $1.7 billion was taken via business email compromise scams, when attackers use spoofed or hacked emails to impersonate a trusted associate and request financial transfers.
http://tiny.cc/e0kpkz
http://tiny.cc/fa9tkz

EUROPE

Norms for responsible state behavior on cyber operations should build on international law

Véronique Christory, the senior adviser for the International Committee of the Red Cross (ICRC), made a statement released on February 11 about "developments in the field of information and telecomunications in the context of international security." Reiterating the discussion paper published in November 2019, the ICRC's perspective is unequivocal and coherent with the UN General Assembly, asserting that the future set of rules on the state

cyber activities are tightly connected and fall under international humanitarian law (IHL). Christory also stressed that achieving general assent to the norms and tenets is an urgent necessity in relation to the ongoing changing field like cyberspace, clarifying that her argument is developed around two rules intended to protect critical infrastructure. Firstly, states must refrain from permitting cyberattacks wittingly aimed at causing damaging or detrimental effects against the functioning of the networked structure that supplies essential services to the population, unless such structure amounts to a "military object." Secondly, states must adopt all the necessary provisions for protecting the critical infrastructures under their jurisdiction from cyberattacks and threats.

http://bit.ly/2wLQwTj

Maze ransomware spree continues amid advisories from French, FBI officials

A hacker group under the name Maze has targeted three legal companies located in South Dakota, threatening to divulge their classified data should they miss paying the demanded ransom. On February 5, the French CERT released a official report about the activity of TA2101, better known as Maze, which was also responsible in previous months for the ransomware against the German governmental authorities and the US taxation field. According to the FBI, Maze represents the latest widespread and malicious cyber-based operations that leverage a ransom often valued at hundreds of thousands of US dollars in order to hit private and governmental companies. In late December, the Georgian manufacturing company sued the anonymous Maze hacking group.

http://bit.ly/2HPVLU2

http://bit.ly/32ncKXo

RUSSIA

Facebook's revelation of fake accounts, linked to Russian military, arises fears in Washington amid coming 2020 elections

According to Facebook, it recently had taken action against malicious actors in Russia that had deployed fake accounts and used other means to manipulate social media users. A network of accounts with links to the Russian military focused its efforts on Ukraine and other neighboring countries. The Kremlin-aligned campaign relied on private messages to steer pro-Russian narratives to influential social media users. The revelation that Russia, in particular, continues to try to weaponize the social media networks is likely to unnerve US leaders. Many in Washington fear that the Kremlin could take aim at the 2020 Presidential elections, much as its "online army" did four years ago.

https://wapo.st/32vxT1H

Russia runs amok on major social networks

A Moscow court fined Facebook with four million rubles for violating Russian legislation on the protection of personal data. Although the new Russian law "On Personal Data" went into force on September 1, 2015, according to which information about Russian users of social networks must be stored on Russian territory, Facebook still has not complied. The Russian "Roskomnadzor" has repeatedly approached the network's headquarters, located in California, demanding to localize the data of Russian users inside Russia. The appeals, according to Russia's authorities, remained unanswered. On the same day, Twitter was fined with 4 million rubles for the same charges. In 2016, due to non-compliance with the law, LinkedIn, the social network of professional contacts, was blocked in Russia.

http://bit.ly/2TkK90F

http://bit.ly/2T6khGM

Russian cyber hacking groups acknowledged as the fastest in the world and they are getting better

Russian hacker groups are the fastest successful data breach attackers, according to the 2019 Global Threat Report from CrowdStrike. Russian nation-state actors, known colloquially as the "bears," have the fastest breakout times by an incredible margin. According to the report, the Russia-based hackers are almost eight times as fast as their nearest competitors. While the Russian "bears" took an average of just 18 minutes and 49 seconds to start moving laterally into other network systems, the North Korean nation-state "chollimas" took two hours and 20 minutes to breakout. The Chinese "pandas" were third fastest in four hours and 26 seconds followed by the Iranian "kittens" with a breakout time of five hours and nine minutes. According to CrowdStrike analysts, Russia will continue to use cyber capabilities to gain situational awareness of neighboring states and rivals further afield.

http://bit.ly/3cfSRWP

Fears rise as Russian planned meddling in 2020 US elections through social networks and hacking is under way

Reports on the intelligence assessments that Russia has launched new efforts to help reelect Donald Trump mark the return of a recurring nightmare for the United States just nine months before the presidential election. The uproar over the new claims suggests that the alleged operation is again delivering for Russia on its intended goals: sowing distrust in the US system and turning Americans against themselves in a way that weakens national unity. Signs of Russian hacking, social media meddling, and attacks on US infrastructure and the resulting confusion and controversy in Washington raise a sobering possibility.

https://cnn.it/32BtZEy

http://bit.ly/2VtKNvq

Pentagon reveals that Russian GRU is behind cyberattacks on ex-Soviet Georgia, for the first time linking it to Sandworm cyber group

The leading nations of the West accuse Russian military intelligence, known as the GRU, for cyberattacking Georgia on October 28, 2019 and pledge to hold the Kremlin accountable. It was only now revealed, following comprehensive investigation by Western intelligence agencies, led by the Pentagon, that Russia sponsored a major cyberattack on the former Soviet Republic of Georgia. The attack knocked thousands of government and private websites offline and interrupted television broadcasts. Secretary of State Mike Pompeo and the Pentagon specifically blamed a Russian hacking unit known as "Sandworm," tying it for the first time to the GRU. The Pentagon said the attack is "just one more example of how Russian malign behavior erodes transparency and predictability, undermines the rules-based international order, and violates the sovereignty of its neighbors."
https://wapo.st/2VtSulw

APAC

Coronavirus prompts Verizon to pull out of RSA sponsorship

Due to the global concern of the new Coronavirus, also known as SARS-CoV-2, infecting over 77,000 people, the planners of the RSA conference declared that Verizon and IBM withdrew their registrations for the event. It was also noted that 1.2 percent of the personal registrations were withdrawn and 6 out of 13 businesses cancelling their participations are Chinese. London Breed, the mayor of San Francisco, assured in an official letter that it is unlikely that the Coronavirus will affect the city, although the local authorities are committed to controlling the epidemic. Therefore, he welcomed all the 40,000 expected attendees to the RSA conference, which is considered one of the most important global cybersecurity events. Despite Mr. Breed's comforting words, Facebook decided to call off its attendance at the Global Marketing Summit as the employees' health and safety take precedence. Furthermore, the

cancellation of the Barcelona Mobile World Conference demonstrates the rampant effect of the virus on the high-tech industry and presumedly such negative repercussions will hamper the manufacture and the issue of phones and other electronic devices.

https://cnet.co/2VgtY75

https://cnet.co/32ncRlD

Opportunities for nuclear arms controls engagement with China

On occasion of the 2010 New Strategic Arms Reduction Treaty (New START) between the United States and Russia, the former intends to extend the agreement to China. Although in the short term it is unlikely that Beijing will become party to the New START, China's increasing military potential might prompt it to undertake a different trajectory from the past. Indeed, three main explanations bear out the Chinese future alignment with Washington's proposal on this issue. Firstly, the international strategy leads the two powerful states at issue to preserve a military and political stability based on a balanced rivalry and a reciprocal commitment for observing the essential rules relating to the nuclear weapons. Secondly, the Chinese non-involvement in the Intermediate-Range Nuclear Forces (INF) between the United States and Russia have unintentionally resulted in the freezing of this bilateral agreement because of the Russian complaints of being the sole country legally bound to the constraints upon its nuclear program. A possible new trend on the part of China may contribute to better security and stability in the global setting. Thirdly, in terms of the domestic economy aspect, China has revealed a serious economic recession unlike its prosperous past; hence, its presence on the side of the United States in favor of a concerted arms monitor system is essential in order to avoid having to reinforce its military potential at the expense of its population. Despite the possibility of gaining China's inclusion in the New START, it is a strategic method for dealing with such a delicate matter, including an exhaustive "understanding of the impact of the new technologies [...] on the nuclear deterrent."

http://bit.ly/380lfJe

MIDDLE EAST

Cyber espionage campaign in Middle East, Europe picked up speed after Soleimani killing

Iran-linked hackers recently have been running spear phishing email campaigns against governmental organizations in Turkey, Jordan, and Iraq in a likely effort to gather intelligence. According to Alex Tilley, a senior researcher for Secureworks, spear phishing activity has increased since the killing of Qassem Soleimani, the leader of the Iran's Quds Force. The research aligns with information that the FBI shared with the industry in January, when it warned of an increase in Iranian "cyber reconnaissance activity." The alert highlighted that Iranian hackers could be zeroing in on the defense industrial base, government agencies, academia, and nongovernmental organizations.
http://tiny.cc/yqkpkz

LATIN AMERICA & CARIBBEAN

The first women's congress on cybersecurity will be held

The Latin American Community—LATAM Cybersecurity by Women (CySecbyWomen)—will hold the first congress of women in cybersecurity called "Cybersecurity by Women v 1.0" at the Peruvian University of Applied Sciences (UPC) in San Isidro, Peru. According to Adataliz Castillo, founder of CySecbyWomen, this is a community that seeks the inclusion of women in cybersecurity through increasing research, active participation, and promoting the discipline through education. This congress will have a series of free discussions throughout the day prepared by talented women from Latin America. In addition, the founder pointed out that although the number of women in cybersecurity continues to be lower than that of men, more women in the industry are advancing to leadership positions compared to their counterparts. The event is sponsored by UPC and brands related to computer security and technology such as ESET, Fortinet, and Open Sec. The talks will

include topics such as pentesting-playground, risks of the internet-of-things, detection of attacks, biometric system, and smart house choices.
https://tinyurl.com/sg9l49n

The cybersecurity challenge

Computerization and cybersecurity should go hand-in-hand in the context of policy development in Cuba, but Cuba lags behind, as a result of a lack of knowledge by users. Dissatisfaction of Cuba's network of technologies, software, and hardware has resulted in the lack of protection against computer crimes, which during the second half of last year was addressed by a set of regulatory norms aimed at supporting the Integral Policy for the Improvement of the Computerization of the Society in Cuba. According to Pablo Ávila, a specialist of the Office of Control of the Ministry of Communications of Cuba, in 2019, the Decree Law 370 was inaugurated, which establishes how to comply with society's computerization policy and addressed issues related to government and electronic commerce and strategies toward companies and organizations around computerization and cybersecurity. "Decree Law 370 is accompanied by two decrees, an agreement of the Council of Ministers and six resolutions of the Mincom, which make up the regulations, to promote the development and use of ICTs and confirm the right, access, and participation of all Cubans in its implementation," according to Ávila. The law includes a range of monetary penalties and potential suspensions of operating licenses, including regulatory mechanisms aimed at ensuring cybersecurity.
https://tinyurl.com/wec2jal

Cybersecurity must be strengthened: Herrera

Mexico's Secretary of the Treasury Arturo Herrera recognized that the federal government should strengthen its cybersecurity to prevent hacking. The official said that the agency in his charge has the necessary protections to deal with an eventual attack. According to Herrera, the real threat facing global financial stability is due to cybersecurity, so not only public agencies

must be protected but also private institutions. After being questioned about the possibility that the Mexican government would acquire new technology to avoid further interference or hacking, Herrera said that measures are taken on a daily basis for this. Recently, a cyberattack affected at least sixty servers of the Ministry of Economy, partially paralyzing its activities. Although the agency assured that the attack did not compromise its services, it published an agreement to suspend procedures.

https://tinyurl.com/s22rzt4