Global Cyber Bi-Weekly Report by INSS 15 November, 2019

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

Contributors: Simon Tsipis, Donal Byrne, Thomas Abma, Lea Abramski

ISRAEL

Israeli and US armies conduct cyber battlefield exercise

The annual joint cyber defense exercise "Cyberdome," gathering IDF and US Cyber Command units, just took place in the United States. This year, it was organized and led by the Cyber Defense Brigade, along with members of the Intelligence Directorate, IAF, Navy, and the Israeli Ground Forces. The seminar consisted of training both countries' special teams to protect operational processes against cyber common challenges, while preserving operational freedom and ensuring supremacy in the cyber domain. The commanding officer of the Dimension Center in the Cyber Defense Division who led the exercise commented that "the exercise reflects the intimate and strategic partnership between the nations and militaries within the field of cyber defense." Indeed, this special training is part of a wider initiative between the C4i and the Cyber Defense Directorate and the US Command, intended to intensify the close partnership between the United States and Israel in the field of defense in the cyberspace.

https://bit.ly/2QlpABw

Israeli robotics delegation to Dubai marks warming Gulf ties

Israel's Prime Minister Benjamin Netanyahu congratulated the Israeli delegation to the unofficial "Robotics Olympics," a robotics competition taking place in Dubai. This greeting followed his visit to the emirate, both showing an intensifying and open relationship between the two countries. The team of Israeli teenagers and their coaches participated in the tournament, gathering more than thousand students from 190 countries. The UAE, like most of the Arab countries, does not have official diplomatic relations with

Israel, but it has been trying to expand its relations with the West and show a more progressive image of the country. For example, the emirate marked the year as the "Year of tolerance," which included interfaith events, attended by rabbis. Authorities allowed Israelis to visit and the Israeli national anthem was played. Next year, the UAE will host "Expo 2020" in Dubai where an Israeli pavilion is expected to be organized. The competition can be regarded as a dry run for further gatherings fostering normalization between Israel and the Arab countries.

https://bit.ly/32KqY3a

https://bit.ly/2qUJQiq

No Israeli government involvement in NSO's alleged Whatsapp hack, minister says

Zeev Elkin, a member of Israel's security cabinet and minister for Jerusalem affairs, stated that the Israeli government was not linked in any way to the alleged hack by the Israeli cyber security company NSO Group. This statement comes shortly after NSO Group was sued by WhatsApp for selling services to its customers that aimed to hack users' devices and access their personal data through the "Pegasus" malware. Back in May 2019, the Financial Times released a report exposing the NSO Group's activity. The company responded that it was only selling a technology enabling states to "fight crime and terror." This breach into the communication app has allegedly affected 1,400 users around the world. Even though the NSO Group denied the accusation, WhatsApp claims that the cybersecurity company took advantage of a vulnerability in its video-calling feature to break into users' devices and supposedly collect data to their clients. Elkin's comments come as Indian journalists and lawyers, whose devices were hacked via the communication platform, wrote a letter asking Prime Minister Narendra Modi to disclose the details of its relationship with the Israeli cybersecurity company. The open letter specifically holds the government accountable on whether public money was used to set up surveillance on a group of Indian intellectuals.

While it is still not verified who used the spyware product to break into users' devices, the software is sold exclusively to governments.

https://bit.ly/2CKlIBZ

https://bit.ly/2Oc72AW

UNITED STATES

Amazon files paperwork for protest of Pentagon's JEDI cloud award

Amazon Web Services (AWS) has filed in the US Court of Federal claims protesting the Pentagon's decision to award its Joint Enterprise Defense Infrastructure (JEDI) cloud contract to Microsoft. AWS CEO Andy Jassy alluded to political pressures behind the decision, further stating, "I think when you have a sitting president who's willing to publicly show his disdain for a company and the leader of a company, it's very difficult for government agencies including the DoD to make an objective decision without fear of reprisal." The JEDI deal is worth an estimated $10 billion over a decade.

http://tiny.cc/bfeegz

Here are some new tools coming to protect the supply chain

Technology used in the Pentagon was discovered to be vulnerable to cybersecurity risks in cases in which the company that either sold or manufactured part of the product was compromised. The Department of Defense (DoD) did not announce with which company it is working to mitigate the vulnerability and in which department the product was used. DoD Deputy Chief CIO Michele Iversen described some of the organization's efforts to protect its supply chain, such as in creating supply chain illumination and decision support tools. The National Institute of Standards and Technology is also developing a "supplier inter-dependency tool to look at different suppliers and their criticality to allow for government to be more effective in asking for capabilities during the procurement process."

http://tiny.cc/medegz

Here's the new plan for election cyberthreat notifications

The Office of the Director of National Intelligence, FBI, and Departments of Homeland Security and Justice released a framework stating that "when an intelligence community agency or DHS' Cybersecurity and Infrastructure Agency wants to send out an alert, the final decision will be 'informed' by a group of experts from different IC agencies." The document emerges as the topic of election security intensifies, resulting in the federal government announcing its notification protocol concerning Congress, state and local governments, as well as the public of election interference operations from foreign adversaries. According to the document, the director of National Intelligence (DNI) will convene a meeting for "broad" public notifications to decide if they should be made. For "nonpublic" notifications that are not required by law to be released, Department of Homeland Security's Cybersecurity and Infrastructure Agency (CISA) or the FBI will notify owners of the critical infrastructure or information.
http://tiny.cc/30degz

Rogue Trend Micro employee exposes customer data

According to the cybersecurity firm, an employee sold the personal information of an estimated 70,000 customers out of 12 million customers to a third party. The incident was uncovered when customers began inquiring about phone calls from scammers posing as Trend Micro employees. The customer database associated with users of its home security software was breached around August. Trend Micro announced the termination of the employee as well as the disabling of the unauthorized account access. The case brings to light the emerging promotion of the "data-centric security model." According to solutions architect Warren Poschman, "instead of just building virtual Maginot lines around data, organizations need to adopt a data-centric security model to protect the data inside from either external or internal threats—in other words, protect what matters most inside as well as you do to protect the outside perimeter."

https://tiny.cc/upxdgz
https://tiny.cc/eqxdgz

EUROPE

UK Labor Party hit by cyberattack ahead of election

The Labor Party, Britain's largest opposition party, said it was subject to a large-scale cyberattack on its digital platforms. The timing is striking, just two weeks before a national election. The party is confident that no data breach occurred. Security services had previously warned about cyberattacks by Russia and other countries, as well as for divisive political campaigns on social media. A security official with knowledge of the matters said the attack was short-lived and a relatively unsophisticated attempt was made to take down some of the party's websites by flooding them.
https://reut.rs/2QhHEw2

European tech investor Balderton launches $400 million start-up fund

European venture capital firm Balderton Capital is launching a $400 million fund in technology start-ups, bringing its total funds under management to $3 billion. A managing partner at the firm said that "Europe has the potential to build the next generation of technology giants . . . we are seeing more and more exceptional founders." The firm's current portfolio includes Healx, which uses artificial intelligence to accelerate treatments for rare diseases, as well as digital accountant provider Revolut.
https://reut.rs/2ObfEYl

Dutch court orders Facebook to pull financial fraud adverts

A court in the Netherlands has ordered the removal of advertisements that misuse the likeness of a local celebrity to promote fraudulent Bitcoin-related investments. The suit demanded that the company take measures to prevent

the issue from reoccurring and that information regarding the scammers be handed over to the victim in case, Dutch billionaire tycoon John de Mol. Facebook's argument that it is just a neutral funnel for information and that it therefore cannot be obliged to act was deemed unacceptable by the court.
https://reut.rs/2NKfGrn

RUSSIA

Russian sovereign internet law—a signal of Kremlin's anxiety from civil revolt

The Russian "sovereign internet law" gives Russian authorities the capability to shut-down the internet coverage in the entire Russian territory. This law has greatly enhanced the Kremlin's control over the internet, in order to avoid any major civil-revolts, which apparently are sweeping all over the globe—a clear signal of the Kremlin's concerns that such a development could occur in Russia. The law was passed earlier this year and allows Russia's government to cut off the internet completely or cut it off from traffic outside Russia "in an emergency." Such technology allows the state telecommunications watchdog to independently and extra-judicially block access to content that the government deems a threat.
https://n.pr/379QF0m

Russia tests new social-network manipulation techniques to be used in US 2020 elections

According to Facebook, it has discovered few "influence networks" on its platforms, apparently backed by Russian authorities and directly connected to the "troll-factory" of Russian oligarch and Putin's "gray cardinal," adviser, Yevgeny Prigojin, who is also considered the owner of the Russian private military company "Vagner" and directly involved with meddling in the US 2016 presidential elections. These Facebook networks-of-influence pages, according to the specialists, were directed at the African continent and, in particular, toward influencing civil opinion in such states as Mozambique,

Cameroon, Sudan, and Libya. Facebook specialists opine that Russia has been testing new disinformation tactics in an enormous Facebook campaign in parts of Africa, as part of its evolving manipulation techniques ahead of the 2020 American presidential elections.
https://nyti.ms/340Wlbe

Putin launches the artificial intelligence development project

President Vladimir Putin approved a National Strategy for the development of "artificial intelligence" until 2030. "In order to ensure the accelerated development of artificial intelligence in Russia . . . I decide to approve the attached National Strategy for the Development of Artificial Intelligence for the period until 2030," the president's decree says. The company that "won" the tender for the development, on behalf of Russian Federation, is the "Russian Direct Investment Fund" (RDIF), which was established in 2011 and is owned and managed by Dmitry Medvedev and Vladimir Putin. From 2016, this fund was appointed by a special presidential decree as a "sovereign fund of Russia."
https://bit.ly/35b212p

APAC

United States to extend license for companies to continue business with Huawei: sources

A two-week extension in addition of the initial ninety-day time frame, is set to be issued to US companies that conduct business with telecommunication giant Huawei Technologies. The extension is not final "due to regulatory hurdles." The "economic blacklist" of the Chinese company began in May, due to concerns of national security. The extension is grounded by American "rural carriers . . . dependent on Huawei for 3G and 4G networks." The time allowance arises as trade discussions come underway between the United States and China.
https://tiny.cc/nmbegz

Cost of cyberattack on Asia-Pacific ports could reach $110 billion

Insurance company Lloyd's of London, in cooperation with the University of Cambridge Center for Risk Studies and the Cyber Risk Management (CyRiM) project at Singapore's Nanyang Technological University, has simulated cyberattacks against the maritime ports of the Asia Pacific region, home to nine of the world's top ten container ports. The projected costs of a cyberattack are estimated at $110 billion.

https://bit.ly/2Qn7D5z

A first, America co-hosts cyber war game "CODE" with Taiwan

The biennial Cyber Offensive and Defensive Exercise (CODE) is being co-hosted by Taiwan and, for the first time since its commencement in 2013, by the United States. Representatives from Australia, the Czech Republic, Indonesia, Japan, and Malaysia, in addition to six other nations will be participating in the multinational cybersecurity exercise, consisting of "simulated attacks on the Taiwan's public and private cyber infrastructure." The acting director of the American Institute in Taiwan, Raymond Greene stated that "the exercise marks a new frontier in the ever-deepening cyber cooperation between the United States and Taiwan." Greene further added the speed of cyberattacks is "increasing exponentially and represent an existential threat to the international rules-based economic order," largely attributed to North Korea and mainland China. Howard Jyan, the director general of Taiwan's Department of Cyber Security, noted that the government's networks are scanned 200 million times and suffer 30 million attacks a month from outside its borders, with China suspected of being responsible for half of these.

https://tiny.cc/pnydgz

MIDDLE EAST

Tunisia's Central Bank denies reports claiming it issued an e-dinar

The Central Bank of Tunisia denies reports that it was launching a national digital currency and claimed the rumors were completely unfounded. Besides, the bank confirmed it was considering the creation of a central bank digital currency (CBDC) but said it was also looking at other alternatives without formulating an immediate project. The bank explained to be very aware of the risks of CBDC or any kind of financial digitalization could imply in terms of "cyber security and financial stability." One of the media agencies that participated in spreading the rumors was the Russian news agency Tass, which reported that the Tunisian Central Bank was leading a joint project with the Universa Blockchain to design and launch a digital currency, announced at a Forex Club Tunisia event. Tunisia's Central Bank has denied this statement, highlighting that the event was actually the main cause of this fake news.
https://bit.ly/376fHxy

Twitter suspends accounts of Palestinian Quds News Network

Several accounts associated with Hamas and Hezbollah have been suspended by Twitter. Raja Abdulhaq, the co-founder of the Quds News Network, one of the suspended accounts, described the suspension to the Wall Street Journal as a clear censorship of Palestinian voices. The news outlet had hundreds of thousands of followers and was apparently considered a source of news on Palestine. This event follows the shutdown of several media websites a few weeks ago that were considered a threat to the stability of the Palestinian Authority. Journalists denounced this decision as an attempt to censor Palestinian voices and called Twitter to cancel the suspension of these accounts. Facebook also restricted Palestinian accounts, which is considered by Palestinians to be pro-Israeli behavior on behalf of the company. The activists also claimed that there was a large gap between the Palestinian Authority and Israel regarding freedom of expression on the internet, with the

social media companies supposedly pressured by Israel. Moreover, Twitter has intervened in a context in which social media giants face strengthened control from lawmakers regarding what they can allow on their platform.
https://tcrn.ch/373tN2y
https://bit.ly/33LJ2LC

Hacked Moroccan lawyer urges action against cyber spies

Abdessadak El Bouchtaoui, a Moroccan human rights lawyer, has called for international protection against cyber spies after his phone was hacked by the Pegasus malware allegedly launched by NSO Group to collect data on more than 1,400 users through a WhatsApp breach. In 2018, he was sentenced to twenty months in jail for insulting authorities and inviting unrest in Morocco, which led him to flee the country for France where he was given asylum. He calls for human rights organizations to protect human rights activists around the world, especially in countries where they can be targeted by the regime as potential political threats. He emphasized the importance of the internet in the activity of the human rights defenders and in preventing against the new threat of cyber spies. The NGO Amnesty International stated that El Bouchtaoui might have been a target of the Moroccan government's surveillance because of his implication with the Hirak movement, but it has no evidence to confirm its suppositions.
https://reut.rs/354BG65

Saudi Arabia recruited Twitter employees to spy on opponents, US prosecutors say

US prosecutors accused Saudi Arabia of recruiting Twitter employees to spy on thousands of accounts, including dissidents. The complaint was released in the US District Court of San Francisco and highlighted a coordinated strategy designed by Saudi officials at the higher level, eventually linked with Crown Prince Mohammed Bin Salman, to recruit Twitter employees to collect users' private data. The two alleged actors of this operation, Ahmad Abouammo, a US citizen, and Ali Alzabarah, a Saudi citizen, were supposedly working for the

Saudi government and rewarded with luxury gifts and significant amounts of money. They were charged for being agents of Saudi Arabia without registering with the United States. The effort allowed the two agents to access user data of around 6,000 Twitter accounts, according to investigators. This proceeding intervenes at a time the regime founds itself very criticized on social media. Moreover, Twitter constitutes the main platform for people in the country to communicate and express their views with relative freedom. Saudi Arabia remained silent regarding this recent disclosure as well as the tech giants Google, Facebook, and Apple, which did not comment the event.
https://bit.ly/37bmQwD
https://tiny.cc/4qxdgz

LATIN AMERICA

South American air forces focus on cybersecurity

South American air force chiefs have sought mutual solutions to current cyber and space security challenges. The South American Air Chiefs and Senior Enlisted Leader Conference was held at Davis-Monthan Air Force Base in Tucson, Arizona, in November 2019. It included more than fifty attendees, including members of the air forces of Argentina, Brazil, Chile, Colombia, Ecuador, Paraguay, and Peru while also including representatives from the US Air National Guard's State Partnership Program and different units of the US Air Force. In an opening speech at the conference, Maj. Gen. Croft said "Our shared neighborhood is currently experiencing some challenges . . . and these challenges compounded with malign states and actors in the region are threatening our democracies and our shared values." The meeting included presentations about the capabilities of each air force in the area of cybersecurity, their advances in space and cybersecurity, and transnational threats. The air chiefs conducted bilateral meetings, along with a guided visit to the 309th Aerospace Maintenance and Regeneration Group and to the System of Cooperation Among the American Air Forces. Lieutenant General Juan José Janer, commander of the Aerospace Command of the Argentine Armed Forces' Joint Chiefs of Staff said that "space and cyber security are two

factors that can spread different aggressions or threats in the world and end up affecting the interests of a nation; that's why every state has the right and responsibility to protect its citizens, their property, and their valuables from these potential threats." He and all speakers emphasized the need for states air forces in the region to collaborate more together in tackling cybersecurity threats.

http://bit.ly/2Xpepcw

Google to build a second data center in South America

It is expected that Google will build a second data center in Latin America in Uruguay, in addition to the one it already has in Chile. It is hoped that the new facility will be located within Uruguay's Science Park in the Canelones area, over a twenty-hectare area that lies in a duty-free tax zone. Planning permission was granted to Google and for the site last month. This will be Google's fourteenth hyperscale data center, joining the others it has in the United States, Europe, Asia, and Chile. Google is believed to have privately confirmed its decision to build in Uruguay in 2017, after a subsea telecoms cable was installed between the Uruguayan beach resort of Punta del Este and the city of Fortaleza in Brazil. The vital loop to the United States is complete with the existence of a subsea cable landing between Fortaleza and Boca Raton in Florida, where key communications players and enterprises can connect across North America and beyond. The value of the data center to be built by Google in Uruguay has so far not been made public.

http://bit.ly/2NOxEZQ