Global Cyber Bi-Weekly Report by INSS 1 December 2019

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

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

ISRAEL

Iranians use Israeli app Waze in recent round of protests

After the announcement of the Iranian government regarding its decision to almost double gas prices, demonstrations have been organized all over the country. Protesters used social media to share information about the riots and several communication platforms were used to intentionally create traffic jams. According to the Italian newspaper La Repubblica, the Israeli app Waze was one of the main tools used by protesters to maximize the impact of the demonstrations in Tehran. Despite the shutdown of many communication websites by the regime to prevent people from communicating with each other and from demonstrating, the Iranians managed to use Waze to calculate where to leave their cars in order to amplify the level of disruption caused by traffic jams.

https://bit.ly/2OV7ZOx

https://bit.ly/2OsKn4Q

How Israel and Facebook are working together to connect the world

According to Maayan Sarig, the communications manager at Facebook, Israel and Facebook are working together in the foreground to make data accessible to the greatest number of people. Indeed, the Facebook representative highlighted the creation of Facebook Lite, specially designed for low-speed connections and low-spec phones. This invention, the product of an Israeli innovation, is sweeping emerging markets, which will soon account for around 90 percent of mobile subscribers. Connectivity in areas of

developing markets can be quite slow and 2G networks are preferred over 3G networks. Facebook Lite can be used on a 2G network and is very similar to the regular version of Facebook, offering almost the same functions. The size of the app is smaller, allowing lower costs and bigger audience. Since the launch of Facebook Lite, many improvements have been made, making it more attractive. This Israeli innovation apparently fostered other companies to follow the path and start designing lite versions of their apps, such as Twitter.
https://bit.ly/35ILQtr

NSO employees take Facebook to Israeli court to unblock accounts

After Facebook sued the Israeli cyber security company NSO Group a few weeks ago, employees from the accused firm filled a complaint with an Israeli court, arguing that the social media platform had blocked their personal accounts in retaliation for the company's deeds. Indeed, the group of employees asked the Israeli court to order the restoration of their Facebook and Instagram accounts, claiming that the company had blocked them without noticing and in spite of Facebook's policies and duties regarding their users. The complaint appears as a response to the lawsuit against the Israeli NSO Group, which was accused of human rights abuses (the Computer Fraud and Abuse Act) through the alleged usage of a spying malware collecting personal data. Since the group of employees starting to complain, Facebook has already unblocked several accounts.
https://bit.ly/33pr6VR

UNITED STATES

A new rule could allow one department secretary to ban certain tech buys

The Department of Commerce recommended a rule which would enable the administration of a government department to halt the acquisition of risky

foreign technology. The regulation includes a set of procedures to "identify, assess, and address information and communication technology (ICT) transactions . . . deemed risky to national security." The suggested guidelines emerge after President Trump gave the authority to moderate or diminish transactions that involve ICT technology provided by bodies located in adversarial states. According to the Department of Commerce, transactions will be appraised per case, taking into account a "fact-specific approach." Secretary of Commerce Wilbur Ross stated that "these rules demonstrate our commitment to securing the digital economy, while also delivering on President Trump's commitment to our digital infrastructure."
https://bit.ly/2DyZDa4

New details emerge on a nearly $1 billion cyber contract

The US Army released information regarding its new approximately $1 billion cyber training contract. The new data concerns the Persistent Cyber Training Environment (PCTE)—in the prototype stage—the main component for the Cyber Training, Readiness, Integration, Delivery and Enterprise Technology (TRIDENT) contract, designed to strengthen "an integrated and robust training environment." The document describes new components, such as the training services extending beyond Cyber Command to the joint services. "It is expected that a single vendor will be selected for TRIDENT, serving as the integrator for various efforts that will be strung together to make up PCTE." The document further mentioned the "management, maintenance, and services the contractor . . . provide for PCTE."
https://bit.ly/2P02rlB

This Senate bill helps states with cybersecurity

Recently a bill was unanimously passed, referred to as the State and Local Government Cybersecurity Act. The statute is meant to increase cybersecurity coordination between states and Department of Homeland Security (DHS) through the department's National Cybersecurity and Communications Integration Center (NCCIC). The bill would facilitate the NCCIC to provide

state and local officials with access to security tools and other resources, as well as ability to participate in joint cybersecurity exercises. "The legislation would also build on previous work by the Multi-State Information Sharing and Analysis Center in preventing and responding to cyberattacks."
https://bit.ly/2R8j416

Trump's national security adviser warns Canadians against Huawei 5G tech

Robert O'Brien, President Trump's national security adviser, warns Canada from authorizing China-based Huawei to build its 5G telecommunications networks, stating that "they're going to know every health record, every banking record, every social media post; they're going to know everything about every single Canadian." The United States threatened that their intelligence-sharing could be affected if Canada follows through, specifically referring to an alliance known as "Five Eyes," composed of the United States, Canada, and other English-speaking countries. The United States has warned other Western nations about the espionage capabilities of China and specifically Huawei.
https://bit.ly/2OBz22b

EUROPE

European Cybersecurity Agency publishes report on smart car security

The European Union Agency for Cybersecurity (ENISA) published a report on the cybersecurity of smart cars. The report aims to promote cybersecurity for connected and (semi-)automated cars by identifying emerging threats and issuing guidance on potential security measures that can help mitigate them. Researchers note that Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) interfaces, needed for deployment of intelligent transport systems and autonomous cars, have expanded the potential attack surface and attack

vectors. Consequences are likely to be beyond the realm of loss of sensitive personal information and could pose a threat to user safety.
http://bit.ly/2XRlQcw

France will not exclude China's Huawei from 5G rollout: minister

Contrary to the position the United States has taken, France will not exclude China's Huawei from its next-generation 5G network but will have the power to vet all equipment makers for any potential security threat. The kickoff of the long-awaited sale of the 5G on Thursday by French telecom regulator Arcep brought an end to months of debate between France's telecom operators and authorities on how to best deploy the new ultra-fast mobile internet technology.
https://reut.rs/2On2HMp

EU countries fail to agree on privacy rules governing WhatsApp, Skype

EU efforts to create ePrivacy regulation that would ensure that tech companies that offer online messaging and email services would be subjected to the same tough rules as telecom providers have failed. Member states did not manage to come to an agreement on the scope of the proposed rules. The problem lies in the complexity of issues regarding rules for cookies, provisions on detecting and deleting child pornography, and consent requirements. These regulations would even the playing field between traditional telecom providers and Facebook's WhatsApp and Microsoft's Skype.
https://reut.rs/2OpxAQr

RUSSIA

Russian "sovereign internet" law: preparing to cope with civil revolt

Russian government is expected to tighten state control over the global network within Russian territory, using the "sovereign internet" bill, which was approved in November. It will strengthen government oversight of the country's cyberspace, activists and specialists say. The legislation aims to route Russian web traffic and data through points controlled by state authorities and to build a national Domain Name System to allow the internet to continue working even if Russia is cut off from foreign infrastructure. This measure definitely comes as a civil revolt-proof tactic. In recent years, Russian authorities have adopted stricter regulations on public protests, tightening their control over society and effectively giving more powers to President Vladimir Putin and points to his growing concern of a possible civil uprising in Russia.

https://wapo.st/2skrWq5

Russian intelligence might have hacked US embassy communication lines

"There is little doubt that the US Ambassador to the European Union Gordon Sondland's cell phone call to President Donald Trump from a restaurant in Ukraine this summer was intercepted by Russian intelligence services," US cyber security officials say. The Russians maintain a particularly large intelligence presence in Ukraine and are known to target the communications of US officials.

The call occurred on July 26, according to Taylor, the day after Trump's phone call with Ukraine's President Volodymyr Zelensky, which prompted a whistleblower complaint alleging Trump solicited "interference" from a foreign country to help his 2020 presidential campaign. "All communications devices of all senior government officials are targeted by foreign governments. This is not new," Bryan Cunningham, executive director of the Cybersecurity Policy and Research Institute at the University of California-Irvine, told CNN last year. "What is new in the cell phone age is the ease of intercepting them," Cunningham added. "Of course, calls are only secure if both parties use a secure device."

https://cnn.it/2Orgkdr

The new Russian hacker group that was discovered appears the most dangerous of all

New revelations suggest that much of that global, Russian-sourced, "cyber-chaos" is not just related to Russia's Military Intelligence Agency, the GRU, but to a single group of hackers within the agency known as Sandworm. "This group is tasked with the most aggressive behavior we see from Russia, and possibly the most aggressive we see, in general," says John Hultquist, the director of intelligence analysis at security firm FireEye, whose team discovered and named Sandworm in the fall of 2014. According to the specialist, this group runs a gamut of cyberattacks, from election interference to technical disruption of the power grids. The GRU has long been suspected of responsibility for the breach that leaked nine gigabytes of emails from the campaign of French presidential candidate Emmanuel Macron just before the French election in early May of 2017—nearly a year after carrying out a similar campaign against the Democratic National Committee and the Clinton campaign in the United States. Now one fresh data point from security firm FireEye ties that operation directly to Sandworm, and specifically to the "NotPetya" malware that later hit Ukraine and spread globally just a month after the French election.

http://bit.ly/2shFUsP

Putin is desperate to bring his hackers, arrested outside Russia, back home

What separates the case of Russian hacker Burkov, arrested by Israel and extradited to the United States, from run-of-the-mill online financial fraud, is the geopolitics that have unfolded since arrested in Israel nearly four years ago. Vladimir Putin's Russia, which in recent years has become ground zero for harboring cybercriminals, has begun aggressively fighting to protect hackers who get caught overseas. At the request of the US Justice Department

and the Secret Service, which had been chasing the leader of the CardPlanet's hacker group, Israel originally arrested Burkov when he was vacationing in Israel in late 2015. It was an early catch in what has become a rising trend of Russian hackers caught while traveling outside Russia, often on vacation. Most recently, in a case that still has US officials scratching their heads, one of the Internet Research Agency employees indicted by special counsel Robert Mueller for interfering in the 2016 presidential election was actually arrested in Belarus—not typically a country friendly to Western law enforcement—but then released and returned to Russia, instead of the United States.
http://bit.ly/34uF9Lf

MIDDLE EAST

80 million affected in Iran internet shutdown, experts say

After the Iranian government shut down access to the internet for more than four days, connectivity has been progressively restored. The regime's decision to block internet access to its citizens was in response to large civil demonstrations, apparently triggered by the announcement of a significant increase in gas prices. The shutdown deprived the population of 80 million access to the internet as it aimed to censor online communications and the spread of information, and to prevent the coordination of protesters. NetBlocks, an internet blockage monitor, stated that the restoration of connectivity in Iran covered only between 10 and 20 percent of the territory. The protests, which started on November 15, 2019, in more than 100 cities and engaging thousands of people, were already the target of a bloody repression orchestrated by the Iranian forces, causing at least a hundred deaths according to the NGO Amnesty International. While the Islamic Republic strengthens its response against protesters, several international organizations already have called the regime to end the escalation of violence.
https://bit.ly/37KQ9Gs
https://reut.rs/2L3eUnv

Iran offers bounty for exposing illegal cryptocurrency mining

The Iranian government announced it will offer a reward to anyone noticing a case of illegal mining of cryptocurrency. Indeed, the regime lately legalized the mining of cryptocurrencies and launched measures against illegal use of electricity. Mostafa Rajabi, a spokesman for Iran's Energy Ministry stated that anyone exposing such an illegal use of electricity will receive a reward equal to 20 percent of the discovered damage's recovery. He also said that new regulations will be applied regarding the price of electricity resulting from mining digital currencies. The Iranian official also mentioned the introduction of incentives dedicated to those who use their own power plants for mining.
https://bit.ly/37KnBgo

Afghan government to apply blockchain in country's healthcare sector

The Afghan government announced its decision to integrate the blockchain technology in the healthcare sector. The Ministry of Public Health signed a Memorandum of Understanding (MoU) with Fantom Operations, a blockchain firm. The main purpose of this initiative will be to bring more transparency, in addition to ameliorating the effectiveness and speed in the health sector through digitalization. The project's main functions will be to identify counterfeit medicines and to create digital medical registries and patients' files in hospitals. Indeed, according to the Medicine Importers Union, 40 percent of medicine and medical equipment is imported to Afghanistan illegally. The government expressed a significant concern regarding the low quality and inaccessibility of medicine. Furthermore, healthcare is not the only field in which Afghanistan is willing to introduce this technology, as it has started to develop blockchain solutions for urban development in a joint initiative with the United Nations ("City for All").
https://bit.ly/2L4x0pk

Saudi-UAE agree to build oil refinery and plan to launch joint digital currency

Saudi Crown Prince Mohammed bin Salman and Sheikh Mohamed bin Zayed, the crown prince of Abu Dhabi and deputy supreme commander of the armed forces, met in Abu Dhabi for an official meeting aiming to strengthen relations between the two countries. After an official reception, the two leaders discussed common issues and potential partnerships. Among the several announcements made by Sheikh Mohamed bin Zayed, after the Saudi prince's visit, it was revealed that the UAE and Saudi Arabia agreed on four new coordinated policies and seven strategic initiatives. One of the decisions made is the creation of an oil refinery able to refine more than one million barrels a day. The leader also mentioned a digital project, soon to include the launch of a common digital currency to ease and foster trading between the two economies. The leaders also discussed strategic challenges and security issues, expressing the will to enhance cybersecurity cooperation.
https://bit.ly/2OsWVcg

LATIN AMERICA

As Venezuela's economy struggles, some of its citizens turn to a lucrative gig: cybercrime

The rate of cybercrime is accelerating in Venezuela as the country's deepening economic and political crisis drives thousands into the underground criminal world, according to a report released by IntSights, a global threat intelligence company. IntSights analysts discovered large-scale and sophisticated efforts to steal personal information from people in Latin America who work in a variety of different sectors. They then either sell that information online or use it to collect additional data. The hackers are based in Venezuela and neighboring countries, like Colombia, where many Venezuelan people have sought refugee status. These information-gathering operations are particularly lucrative for Venezuelans as they are sold for cryptocurrency, such as bitcoin, which has endured rapid inflation given the country's economic

situation. Venezuela-based cybercrime efforts span a variety of common digital misdeeds, including large-scale email phishing efforts and malware campaigns. Venezuelans now rely heavily on social media apps, such as Instagram, Snapchat, Facebook and Twitter, as well as the messaging app WhatsApp for information. Cryptocurrencies have become a widely used form of payment in Venezuela. The Venezuelan government created its own digital currency, dubbed the "petro," in February 2018. "The Maduro regime's priorities do not include protecting infrastructure or global enterprises at the moment," the report states.

https://nbcnews.to/2OW5onp

Malware campaign targeting banks in Spain and Latin America

An investigation was conducted by Blueliv, concerning a campaign targeting Latin American and Spanish users. "The immediate objective of the campaign is the installation of a banking Trojan on the users' systems, with the goal of stealing sensitive financial information that can be used to perform fraud." A technical report is available detailing the distribution, email, downloader, banker, and other details surrounding this campaign. In this malware campaign, it can be detected when the user is operating with their online banking account. "Some of these elements point to an attacker which is not extremely advanced and [most likely] located in Latin America. The modus operandi and tools typically match with Brazilian actors, but also actors located in other South American countries have been seen with a similar behavior."

https://bit.ly/2rH5APl