

Global Cyber Bi-Weekly Report by INSS May 15 2019

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

Contributors: Simon Tsipis, Gal Sapir, Robin Veldwijk, Thomas Abma

ISRAEL

Amnesty International takes legal action against Israeli surveillance company NSO

The human rights organization Amnesty International has filed a petition with the Tel Aviv District Court requesting the Israeli Ministry of Defense to invalidate the accused company's export license. Amnesty asserts that the software of the cyber surveillance company's was utilized in an attempt to conduct surveillance on one of its employees— who is also a Saudi human rights activist. Amnesty first announced the suspected targeting in August 2018, claiming Pegasus technology was used in attempt to infiltrate the staff members calls, messages, and gain remote access of their mobile device; suspecting "information about the organization's members in Saudi Arabia and other countries could have been obtained, resulting in potential risk to their personal freedom and well-being."

<http://tiny.cc/vvin6y>

Israeli startups shine in the \$92 billion cybersecurity market

Israel has emerged as a leader in the cybersecurity industry, with significant growth among startup organizations and maturing companies. There are approximately 450 cybersecurity corporations operating in Israel, and of those, 60 were founded in the past year. The growth of the cybersecurity industry in Israel has also led to a boom in employment among related fields. Job numbers have grown by more than 10 percent in recent years, with around 12,000 Israelis working for cybersecurity firms. The country's position in the market is second to only the United States and is expected to continue its impressive growth pattern. The ongoing tensions in the Middle East are a great reason why Israel is at the top defending against computer or internet-

based attacks. The military's presence and emphasis on data protection are definitely factors as well. A large part of that defense focus is placed on cybersecurity to ensure that national information remains safe.

<https://bit.ly/2Hgb3Sx>

Israel Defense Award winner Professor Ben-Israel joins Cyber 2.0

Prof. Yitzhak Ben-Israel—who serves as chairman of the Israel Space Agency, head of the Cyber Center at Tel Aviv University, and head of the Yuval Ne'eman Workshop on Science, Technology, and Security—was twice awarded the Israel Defense Award for his contribution to national security. He also served as head of the Defense Ministry's Administration for the Development of Weapons and Technological Infrastructure (MAFAT), and associated with the establishment of the National Cyber Directorate, the civilian cyber defense branch within the Prime Minister's Office. Cyber 2.0, an offensive – defensive prevention system, is based on an "unbreachable mathematical chaos model," supposedly capable of preventing the spread of any kind of cyberattacks; within and outside organizational networks. Earlier in the year, the cybersecurity company offered a \$100,000 reward to "any U.S based engineer that could hack the platform," resulting with no victors. According to the newest board member, the cyber solution "...is the only one that can fully address all kinds of attacks." Ben-Israel further states, Cyber 2.0 "...is a groundbreaking solution."

<https://bit.ly/2WlzbCv>

Israel neutralizes cyberattack by blowing up a building with hackers

The tensions between Israel and Hamas have increased over the last year, as the latest conflict began on Friday, May 3, after Hamas militants launched at least 600 rockets and mortars at Israel and shot two Israeli soldiers. At least 27 Palestinians and 4 Israeli civilians have been killed, and over 100 of them have

been injured. The Israel Defense Force (IDF) claims to have neutralized an “attempted” cyberattack by launching airstrikes on a building in the Gaza Strip from where it says the attempted attack originated. “We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work. HamasCyberHQ.exe has been removed,” said the IDF on Twitter. The commander did not reveal the name of the target but did say that the cyberattack aimed at “harming the way of life of Israeli citizens.”

<https://bit.ly/2Yiaz4f>

UNITED STATES

2 Chinese men indicted for hacking Anthem

In what has been coined “the biggest known health care hack in US history” resulted in the breach of an estimated 79 million customers’ personal data from the second-largest insurer Anthem. Information included “names, birthdates, Social Security numbers, and medical IDs.” So far there is no evidence of the data being sold for use of fraud. According to Symantec, the hackers are suspected to be Black Vine, a well-resourced Chinese group, believed to have been conducting cyberespionage and pursuing the US aerospace, energy, and healthcare industries for a few years, although it is not clear if the operation was state-sponsored. In recent developments, two of the associated hackers, Fujie Wang and John Doe were recently indicted by a federal grand jury and were linked to three other hacks of US companies. The former is stated to reside in Shenzhen, China, while Doe’s location is based on his undertakings traced to China; the United States and China do not have an extradition treaty. In October 2018, Anthem agreed to pay the government \$16 million to resolve impending privacy violations.

<http://tiny.cc/gg4l6y>

Cyberattack cripples Baltimore’s government computer servers

After a ransomware virus was detected to have breached the city's network, a great amount of computers were shut down. Mayor Young stated that "police, fire, and EMS dispatch systems have not been affected...[and there is] no evidence that any personal data has left the system." Email and phone outages transpired in parts of the city, inhibiting citizens to pay some utility bills over the phone. This is the second incident since an attack in March 2018, which lead to a "17-hour shutdown of automated emergency dispatching." The FBI's cyber squad is aiding in determining the source and scope of the attack.

<http://tiny.cc/9hcm6y>

Microsoft offers software tools to secure elections

Some of the top US election vendors have stated their positive intent of possibly incorporating Microsoft's "verifiable and more transparent open-source software" into their voting systems. These companies include ES&S of Nebraska, Dominion Voting Systems of Colorado, and Hart InterCivic of Texas, which "control about 90 percent of the market for election equipment." Prototypes of "ElectionGuard" are expected to be available this summer on the horizon of the 2020 presidential elections. Microsoft has partnered with the Oregon-based company, Galois, on the software development project; notably, the latter is also under contract for designing a "secure voting system" with DARPA, the Pentagon's research organization. The product is structured to function either as a standalone product or with utilized election systems, excluding mail and internet systems, and further providing "end-to-end verification of voting, postelection audits, recounts...[and can simultaneously] be used with a ballot-making device...optical scanner... [and] on hand-marked paper ballots." As part of Microsoft's "Defending Democracy Program," company officials stated the product will be free, in addition to giving political parties and campaigns a 75% reduced cost on the Office 365 suite product.

<http://tiny.cc/qr5l6y>

Washington state enacts new data breach notice requirements

Subsequent of Governor Inslee's signing of the bill HB 1071, business in the state now will have 30 days instead of 45 to notify the victims and state attorney general of data breaches. Currently, breach notifications are required only if names, Social Security numbers, or drivers' license numbers are implicated. The law will additionally oblige companies to notify affected individuals if their biometric data or medical history, attached to their names, is breached. The bill expands the definition of "personal information" to include such data, along with full birth dates and health insurance identification numbers, among other changes. Furthermore, companies will have to notify customers how long their data was exposed, and specify to the state attorney general's office the number of Washington residents affected, the types of personal information beached, a time frame for the exposure, and steps the company took to contain the breach. The amendments signed into law will go into effect on the first of March 2020.

<http://tiny.cc/y6dn6y>

EUROPE

SoftBank Vision invests \$800 million in UK Fintech Greensill

SoftBank fund's investment in Greensill, which provides companies with alternative supply chain funding, has increased its value to \$3.5 billion. "Greensill estimates the largely untapped market for working capital finance at \$55 trillion." The money will aid the company's market expansion plans into Brazil, China, and India. In addition, it will support its development of "new technologies to make more capital accessible to its clients" for which the norm of banks is to only offer to few significant clients. "Since 2015, the company has delivered annual growth of more than 100%."

<http://tiny.cc/rq9l6y>

France: G7 countries to simulate cross-border cyberattack next month

For the first time, Western industrial powers will cooperate in a simulation of a trans-border cyberattack related to the financial sector. The mockup drill is organized by the French central bank under France's presidency of the G7 and is scheduled for June. The scenario will play out as a technical component extensively used in the sector that is discovered to be infected with malware. The three-day exercise will "involve 24 financial authorities from the seven countries, comprising central banks, market authorities and finance ministries."

<http://tiny.cc/k39l6y>

RUSSIA

NATO's cyber military drills in ex-Soviet republics to deter Russia

NATO's recent cyber exercise was conducted in a snow-covered military base in Tallinn, Estonia. The NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) initiated the "Locked Shields"—a massive cyber-defensive exercise that enables cybersecurity experts to enhance their skills in defending national IT systems and critical infrastructure in real-time attacks. Cyber military officials learn how to deal with threats with the help of civilian experts who know the systems inside out. Siim Alatalu, a Strategy Researcher at the CCDCOE, explains that "the targets are things around us in daily lives, anything from traffic lights, to power plants, to gas refineries." Why Estonia? Estonia until today is considered the first sovereign country to have been cyberattacked on a national scale by Russia. The attack of 2007, which has been referred to as the world's first cyberwar, occurred following a dispute due to Estonia's decision to relocate a statue of a Red Army soldier in Tallinn, which Russia assertively opposed.

<http://bit.ly/2vVDyyo>

US Cyber Command to expand in Europe to counter Moscow's cyber warfare

American cyber military officials from the US Cyber Command were deployed last year to Ukraine, Macedonia, and Montenegro. The officials said that their missions included defending elections and uncovering information about Russia's newest abilities. The US Cyber Command will continue some of those partnerships and expand its work to other countries under attack from Russia, officials said. American officials are pushing ahead efforts with allied nations to counter Russia's interference in democratic elections and other malign activities. These efforts intend to allow the United States to better observe and counter Moscow's newest cyberweapons.

<https://nyti.ms/2LDraxO>

FBI: We know that Russia's regime is a state-criminal merger

The Russian government is increasingly partnering with cyber criminals in its online espionage efforts, according to John Carlin, who had been a national security official in the Obama administration. The Russian government is actively engaged with organized cybercrime networks to achieve its political goals. This gives us the "big picture," that the Russian regime is tightly merged with organized crime, and this state-criminal fusion creates a "mafia style" crime family, and "the head of the crime family is Putin," Carlin said. "We, and the FBI believe that such operations enabled Russian military intelligence (GRU) to gain access to the network of at least one Florida county government, in the 2016 elections," stated the redacted report of Special Counsel Robert Mueller.

<http://bit.ly/2Q1AmL5>

APAC

How Chinese Spies Got the N.S.A.'s Hacking Tools and Used Them for Attacks

Symantec, a leading cybersecurity firm, has discovered that Chinese intelligence agents acquired the hacking tools of the National Security Agency (NSA) and repurposed them in 2016 to attack American allies and private

companies in Europe and Asia. This is the latest evidence that the United States has lost control of key parts of its cybersecurity arsenal. Based on the timing of the attacks and clues in the computer code, researchers believe the Chinese did not steal the code but rather captured it from the NSA. Some of those hacking tools acquired by the Chinese were later dumped on the internet by a still-unidentified group that calls itself the Shadow Brokers and were used by Russia and North Korea in devastating global attacks, although there appears to be no connection between China's acquisition of the American cyberweapons and the Shadow Brokers' later revelations.

<https://nyti.ms/2PO0GYK>

Binance cryptocurrency exchange blames hackers in theft of \$40 million in bitcoin

Binance, founded in China, and is currently headquartered out of Japan, is one of the largest cryptocurrency exchanges. The company was recently hit by a "large scale" attack resulting in a loss of 7,000 bitcoin worth nearly \$41 million. Hackers employed phishing and viruses to steal "two-factor authentication keys, API data...", and possibly other information. Binance will use its "Secure Asset Fund for Users, stored separately to cover any losses." This incident falls on the proliferating trend of targeting cryptocurrency exchanges; as in 2018 with Coincheck exchanges, losing \$400 million and in 2016 when "Hong-Kong based Bitfinex" lost \$63.7 million. Reported earlier this year, the UN alleges North Korean hackers with the theft of at least \$571 million from cryptocurrency exchanges.

<https://tiny.cc/lzjo6>

MIDDLE EAST

Turkish watchdog says it fines Facebook fined \$271,000 for data breach

The KVKK, the Turkish organization responsible for protecting personal data, fined the American tech-giant after discovering a bug that allowed third-party

applications to access the photos of Facebook users. According to the KVKK, 300,000 users in Turkey may have been affected by this data breach. According to a statement about the breach by Facebook itself, the bug occurred for twelve days in September 2018. The company did not intervene in time, revealing deficiencies in technical precautions regarding this issue.

<https://reut.rs/2WGXX6e>

Iranian media say reformist magazine closed by authorities

The weekly magazine Seda was suspended from publishing by a court in Tehran, according to a report by the reformist newspaper Arman. Its last front page had shown a US aircraft carrier fleet, along with the caption: "At the crossroads between war and peace." The article went on to warn that closing the strategic strait of Hormuz—through which a third of all oil traded by sea passes—would lead to "widespread war."

<http://bit.ly/2HfZPwc>

Dubai creates Future Council for Blockchain initiative

A "Future Council" has been created as part of the recently launched Dubai Future Councils initiative. Made up of fourteen members from various government and international entities, the council will discuss topics relating to the expansion of implementation of Blockchain technology in both the public and the private sector. Dubai has set out to become the "smartest city in the world and a regional and global Blockchain hub," according to the Council's director Aisha Bin Bishr.

<http://bit.ly/2VjrnFS>

Bahrain's Investcorp agrees sale of cyber security firm for \$515m

Investcorp has announced the sale of SecureLink Group for €515 million to global telecom group Orange. Acquired in December 2015, the company grew to become one of the largest cybersecurity infrastructures and managed

service providers in Europe. SecureLink Group has seen its revenue more than triple since the start of its partnership with Investcorp, according to Hazem Ben Gacem, co-CEO of Investcorp.

<http://bit.ly/2E4vfEV>